



Administering Avaya Aura[®] System Manager for Release 8.1.x

Release 8.1.x
Issue 10
March 2021

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, <https://support.avaya.com/LicenseInfo> UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, <https://support.avaya.com/LicenseInfo>, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: <https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL

PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com> or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	28
Purpose	28
Change history	28
Chapter 2: Overview	36
System Manager overview	36
New in this release	38
New in System Manager Release 8.1.3.1	38
New in System Manager Release 8.1.3	39
New in System Manager Release 8.1.2	41
New in System Manager Release 8.1.1	41
New in System Manager Release 8.1	42
Log on to System Manager	45
Turning off the compatibility mode	45
System Manager web console	46
System Manager Dashboard field descriptions	48
Logging on to the System Manager web console	49
Change Password field descriptions	53
Logon information for users with administrator privilege	53
Certificate based authentication	54
Tenant Management web console	57
Password and security policies for all administrators	59
Password aging policy enforcement	59
Password strength policy enforcement	60
Password history policy enforcement	60
Password lockout policy enforcement	60
Editing password policies	60
Password policies field descriptions	61
Managing System Manager password through CLI	64
Inactive session termination policy	71
Editing Session Properties	71
Session Properties field descriptions	71
Inactive Account Deactivation Policy field descriptions	72
Security settings	72
Login warning banner	72
Editing the login warning banner	73
Security Settings field descriptions	73
Customized interface	74
Adding the corporate logo	74
Customized Interface field descriptions	74
Reimporting the SSO cookie domain value	75

Administrative users.....	75
Viewing administrative user details.....	75
Adding an administrative user.....	76
Editing administrative user details.....	76
Editing administrative user roles.....	76
Enabling an administrative user.....	77
Disabling an administrative user.....	77
Deleting an administrative user.....	77
Terminating administrative user sessions.....	78
Administrative Users field descriptions.....	78
Add New Administrative User field descriptions.....	78
Chapter 3: Directory synchronization.....	80
Directory synchronization overview.....	80
Results of synchronization from the LDAP directory server to System Manager.....	81
Results of synchronization from System Manager to the LDAP directory server.....	81
Limitations in the synchronization of the LDAP directory server.....	82
Adding the synchronization datasource.....	82
Editing the synchronization datasource.....	84
Deleting a synchronization datasource.....	85
User synchronization datasource field descriptions.....	85
Preferred languages.....	90
Creating the user synchronization job.....	91
Scheduling a user synchronization job.....	92
Deleting a user synchronization job.....	93
User active synchronization job field descriptions.....	93
Synchronization job history.....	93
Synchronization job history field descriptions.....	94
Viewing Job Summary.....	94
Viewing Job Summary field descriptions.....	95
Chapter 4: Geographic Redundancy.....	96
Geographic Redundancy overview.....	96
Licensing in Geographic Redundancy.....	97
Geographic Redundancy terminology.....	98
Geographic Redundancy replication.....	100
Prerequisites for the Geographic Redundancy setup.....	100
Hardware resource and parameter for the Geographic Redundancy setup.....	101
Key tasks for Geographic Redundancy.....	103
Prerequisites before configuring Geographic Redundancy.....	105
Geographic Redundancy prerequisites overview.....	105
Copying the CRL URL.....	106
Configuring CRL download on the secondary System Manager server.....	107
Adding the trusted certificate of primary server to the secondary System Manager server...	108
Configuring Geographic Redundancy.....	109

Enabling the Geographic Redundancy replication.....	111
Disabling the Geographic Redundancy replication.....	112
Activating the secondary System Manager server.....	113
Deactivating the secondary System Manager server.....	114
Restoring the primary System Manager server.....	115
Reconfiguring Geographic Redundancy.....	117
Converting the primary System Manager server to the standalone server.....	119
About the Health Monitoring service.....	119
Configuring the timeout interval for health monitoring.....	120
Geographic Redundancy field descriptions.....	120
GR Health field descriptions.....	122
Prerequisites for configuring disaster recovery.....	124
Disaster recovery prerequisites.....	124
Configuring CRL download on the primary System Manager server.....	124
Adding the trusted certificate of secondary server to the primary System Manager server...	125
Replacing System Manager servers.....	126
Replacement of System Manager servers.....	126
Moving the existing primary System Manager server to a different location.....	126
Restoring the primary System Manager server using the old primary server backup data...	127
Restoring the primary System Manager server using the data on the secondary System Manager server.....	128
Replacing the secondary System Manager server on the site.....	128
Recovering the primary System Manager server from disaster.....	129
Configuring the GR-unaware elements to work with System Manager.....	131
Geographic Redundancy-unaware elements overview.....	131
Elements Geographic Redundancy manageability status matrix.....	132
Configuring various elements to change to the secondary System Manager.....	133
Introduction.....	133
Session Manager configuration.....	133
Communication Manager configuration.....	136
CS 1000 configuration.....	139
Meeting Exchange configuration.....	143
Presence Server configuration.....	143
Messaging configuration.....	144
Avaya Aura® Conferencing configuration.....	148
Avaya Meetings Server configuration.....	151
IP Office configuration.....	154
Visualization, Performance, and Fault Manager.....	157
Application Enablement Services.....	157
Avaya Aura® Contact Center.....	157
Avaya Multimedia Messaging configuration.....	158
Chapter 5: Managing groups and roles for resources.....	159
Managing groups.....	159

Group management.....	159
Viewing groups.....	160
Creating groups.....	160
Modifying groups.....	161
Creating duplicate groups.....	161
Deleting groups.....	162
Moving groups.....	162
Synchronizing resources for a resource type.....	163
Assigning resources to a group.....	163
Searching for resources.....	164
Searching for groups.....	165
Filtering groups.....	165
Filtering resources.....	166
Removing assigned resources from a group.....	167
Group Management field descriptions.....	167
New Group field descriptions.....	168
View Group field descriptions.....	170
Edit Group field descriptions.....	172
Delete Group Confirmation field descriptions.....	173
Duplicate Group field descriptions.....	174
Move Group field descriptions.....	174
Resource Synchronization field descriptions.....	175
Managing resources.....	175
Manage resources.....	175
Accessing resources.....	175
Assigning resources to a new group.....	176
Adding resources to a selected group.....	176
Searching for resources.....	177
Filtering resources.....	177
Resources field descriptions.....	178
Choose Group field descriptions.....	180
Choose Parent Group field descriptions.....	180
Managing roles.....	181
Role Based Access Control.....	181
Built-in roles.....	182
Custom roles.....	186
Viewing user roles.....	187
Adding a custom role.....	187
Adding a custom tenant administrator role.....	189
Assigning permissions to access Solution Deployment Manager.....	190
Mapping permissions by using the template.....	191
Assigning users to a role.....	192
Unassigning users from role	193

Copying permission mapping for a role.....	193
Editing a custom role.....	194
Deleting custom roles.....	194
Roles field descriptions.....	194
Add New Role field descriptions.....	195
Role Details field descriptions.....	196
Add Mapping field descriptions.....	196
Assigned Users field descriptions.....	197
Permission mapping field descriptions.....	197
Chapter 6: Granular role based access control.....	199
Granular RBAC.....	199
Implicit permissions required for Communication Manager objects.....	200
Sample scenario for the range feature.....	202
Assigning permissions in User Management.....	202
Assigning permissions through User Management.....	202
Field-level RBAC.....	204
Endpoints.....	208
Range in endpoints.....	208
Assigning range for endpoints.....	209
Assigning permissions for fields in endpoints.....	211
Hunt Group.....	213
Assigning range for hunt group.....	213
Assigning permissions for fields in hunt group.....	215
Trunk Group.....	217
Assigning permissions for fields in trunk group.....	217
Chapter 7: Managing users, public contacts, and shared addresses.....	219
Managing users.....	219
Users, public contacts, and shared addresses.....	219
Access to administrative users.....	220
End user self provisioning.....	221
Enabling self provisioning.....	221
Disabling self provisioning.....	221
Generating the communication profile password from the self provisioning interface.....	222
Changing the communication profile password from the self provisioning interface.....	223
Viewing details of a user.....	224
Creating a new user account.....	225
Creating a new user profile using the user provisioning rule.....	226
Results of using the user provisioning rule.....	227
Modifying user accounts.....	230
Creating duplicate users.....	231
Removing user accounts.....	232
Removing the deleted users from the database.....	232
Editing users in bulk.....	233

Viewing bulk user edit jobs.....	233
Deleting the bulk user edit job.....	234
Create new profile option.....	234
User Provisioning Rules and User Bulk Editor.....	235
User Bulk Editor field descriptions.....	235
Filtering users.....	247
User searchable fields.....	248
Searching for users by using Search component.....	249
Searching for users by using Advanced Search.....	249
Assigning roles to a user.....	249
Assigning roles to multiple users.....	250
Removing roles from a user.....	251
Assigning groups to a user.....	251
Assigning groups to multiple users.....	252
Removing a user from groups.....	252
Viewing deleted users.....	252
Restoring a deleted user.....	253
Assigning users to roles.....	253
Unassigning users from role	254
Managing addresses.....	254
Managing communication profiles.....	257
Managing default contact list of the user.....	274
Managing private contacts of a user.....	280
User Management field descriptions.....	292
User Profile Add field descriptions.....	295
User Profile Edit <User Name> field descriptions.....	315
User Profile View <User Name> field descriptions.....	333
User Profile Duplicate <User Name> field descriptions.....	348
User Delete Confirmation field descriptions.....	364
Assign Roles to Multiple Users field descriptions.....	364
Assign Roles field descriptions.....	365
Assign Groups field descriptions.....	366
Assign Groups to Multiple Users field descriptions.....	366
Deleted Users field descriptions.....	367
User Restore Confirmation field descriptions.....	368
Assign Users To Roles field descriptions.....	368
UnAssign Roles field descriptions.....	369
Managing bulk import and export.....	370
Managing public contacts.....	593
Manage public contact list.....	593
Adding a new public contact.....	593
Modifying details of a public contact.....	594
Deleting public contacts.....	594

Viewing the details of a public contact.....	594
Adding a postal address for a public contact.....	595
Modifying postal address of a public contact.....	595
Deleting the postal addresses of a public contact.....	596
Choosing a shared address for a public contact.....	596
Adding a contact address of a public contact.....	596
Modifying the details of a public contact.....	597
Deleting the contact address of a public contact.....	597
View Public Contact field descriptions.....	597
Edit Public Contact field descriptions.....	599
New Public Contact field descriptions.....	601
Public Contacts field descriptions.....	602
Managing shared addresses.....	604
Manage shared address.....	604
Assigning a shared address to the user.....	604
Adding a shared address.....	605
Modifying a shared address.....	605
Deleting a shared address.....	605
Add Address field descriptions.....	606
Edit Address field descriptions.....	606
Shared Address field descriptions.....	607
Managing presence access control lists.....	608
Manage Presence Access Control Lists.....	608
Presence ACL field descriptions.....	608
Communication profile password policy enforcement.....	609
Communication profile password policy.....	609
Editing the password policy for the communication profile	610
Communication Profile Password Policy field descriptions.....	611
Chapter 8: Managing user provisioning rules.....	613
User Provisioning Rule.....	613
Capabilities and guidelines of user provisioning rules.....	614
Adding User Provisioning Rules.....	615
Creating the user provisioning rule.....	616
Modifying the user provisioning rule.....	616
Viewing the user provisioning rule.....	617
Creating a duplicate user provisioning rule.....	617
Deleting a user provisioning rule.....	618
User Provisioning Rules field descriptions.....	618
New User Provisioning Rule field descriptions.....	619
Chapter 9: Managing elements.....	629
Importing users from Subscriber Manager to User Management.....	629
User data import to System Manager.....	629
Preparing the Subscriber Manager user data for import to User Management.....	630

Importing the Subscriber Manager user data to User Management.....	631
Subscriber Manager datasource parameters and attributes.....	633
Exporting the user data and creating the user profile.....	634
Importing users from CS 1000 Subscriber Manager to User Management.....	636
CS 1000 Subscriber Manager data import options.....	636
Preparing the CS 1000 Subscriber Manager user data for import to System Manager.....	636
Importing the CS 1000 Subscriber Manager user data to System Manager.....	637
Exporting the CS 1000 user data and creating the user profile.....	637
Preparing the CS 1000 Subscriber Manager user data for import to System Manager.....	637
Importing the CS 1000 UCM Subscriber Manager user data to System Manager.....	638
Exporting the CS 1000 user data and creating the user profile.....	639
Managing messaging.....	639
Messaging Class Of Service.....	639
Viewing Class Of Service.....	639
Class of Service List field descriptions.....	640
Messaging.....	640
Chapter 10: Managing Communication Manager.....	648
System Manager Communication Manager capabilities.....	648
Configuring Communication Manager user profile settings.....	649
Editing the Select All attribute in a table.....	650
Search component for Communication Manager objects.....	650
Managing Communication Manager objects.....	652
Communication Manager objects.....	652
Agents.....	658
Announcements.....	670
Audio Groups.....	682
Holiday Table.....	686
Vector Directory Number.....	688
Vector Routing Table.....	692
Service Hours Tables.....	695
Coverage Path.....	697
Coverage Time-of-day.....	706
Element Cut-Through.....	709
Endpoints.....	711
Hunt Group.....	779
Trunk Group.....	784
Managing Off PBX Configuration Set.....	786
Managing Off PBX Endpoint Mapping.....	789
Xmobile Configuration.....	791
Automatic Alternate Routing Digit Conversion.....	796
Automatic Route Selection Digit Conversion.....	798
Automatic Route Selection Toll.....	801
Cluster Session Manager.....	802

Data Modules.....	804
Class of service.....	814
Authorization Code.....	817
Class of Service Group.....	819
Uniform Dial Plan Groups.....	823
Uniform Dial Plan.....	827
Usage options.....	831
NRP Group.....	834
Chapter 11: Managing backup and restore.....	838
Backup and restore.....	838
/emdata/svars/ backup in System Manager.....	839
Backup failure due to lack of disk space in /swlibrary.....	839
Disk space management for System Manager backup.....	840
Backup and restore on System Manager that is configured for Geographic Redundancy.....	840
Accessing the Backup and Restore service.....	841
Viewing list of backup files.....	841
Enabling backup encryption.....	842
Creating a data backup on a local server.....	842
Creating a data backup on a remote server.....	843
Scheduling a data backup on a local server.....	844
Scheduling a data backup on a remote server.....	844
Editing a scheduled backup job.....	845
Deleting the scheduled backup job.....	846
Restoring data backup from a local server.....	847
Restoring a backup from a remote server.....	848
Restoring the backup through the command line interface.....	849
Disk space required for backup.....	850
Time duration for backup and restore.....	851
Supported ciphers, key exchange algorithms, and mac algorithms.....	851
Backup and Restore field descriptions.....	853
Backup field descriptions.....	853
Schedule Backup field descriptions.....	855
Restore field descriptions.....	856
Chapter 12: Configuring applications.....	859
Managing data retention rules.....	859
Data retention rules.....	859
Excluded log files.....	859
Accessing the Data Retention Rules service.....	861
Modifying data retention rule.....	861
Applying data retention rule.....	861
Data Retention field descriptions.....	862
logRetention command.....	862
updateLogRetention command.....	863

pruneAllLogs command.....	863
Configuring applications.....	864
Configuration management.....	864
View Profile: Agent Management field descriptions.....	864
Configuring IP Office.....	865
IP Office profile field descriptions.....	865
View Profile: Communication System Management Configuration field descriptions.....	866
Edit Profile: Communication System Management Configuration field descriptions.....	867
View Profile: Event processor field descriptions.....	868
View Profile: Configuration field descriptions.....	869
View profile: Inventory field descriptions.....	869
Edit Profile: Inventory field descriptions.....	870
View and Edit Profile Messaging field descriptions.....	871
View Profile: Data Transport Config field descriptions.....	872
View Profile: Data Transport Static Config field descriptions.....	874
View and Edit Profile SMGR field descriptions.....	874
View Profile: Alarming UI field descriptions.....	877
Edit Profile: Alarming UI field descriptions.....	878
View Profile: Common Console field descriptions.....	878
Edit Profile: Common Console field descriptions.....	879
View Profile: GracefulShutdown field descriptions.....	880
Edit Profile: GracefulShutdown field descriptions.....	880
View Profile: HealthMonitor field descriptions.....	880
Edit Profile: HealthMonitor field descriptions.....	881
View Profile: Licenses field descriptions.....	882
Edit Profile: Licenses field descriptions.....	882
View Profile: Logging UI field descriptions.....	882
Edit Profile: Logging UI field descriptions.....	883
View Profile: Logging Service field descriptions.....	884
Edit Profile: Logging Service field descriptions.....	885
View and Edit Profile: SMGR Element Manager field descriptions.....	885
View Profile: SNMP field descriptions.....	887
View Profile: Scheduler field descriptions.....	887
Edit Profile: Scheduler field descriptions.....	888
Configuring the TrapListener service.....	889
View Profile: TrapListener field descriptions.....	889
Configuring Trust Management.....	890
View Profile: TrustManagement field descriptions.....	890
Edit Profile: TrustManagement field descriptions.....	891
View Profile: User Bulk Import Profile field descriptions.....	892
Edit Profile: User Bulk Import Profile field descriptions.....	893
Chapter 13: Managing inventory.....	896
Element management.....	896

Methods to add elements to System Manager.....	898
Manual addition of elements.....	898
Adding a new element.....	898
Bulk import of elements.....	898
Discovering elements.....	899
Working with Elements in System Manager.....	915
Additional information required for creating the Communication Manager or Messaging element.....	915
Manage elements in System Manager configured with Geographic Redundancy.....	915
Determining the System Manager that manages a GR-aware element.....	916
Viewing details of an element.....	916
Modifying an element.....	917
Deleting an element.....	917
Exporting elements from the System Manager command line interface.....	917
runRTSCli.sh command.....	918
Assigning elements to an element.....	919
Removing assigned elements.....	920
Managing access profiles and ports.....	920
Managing and unmanaging elements from System Manager.....	922
Adding Platform type elements to System Manager.....	923
Adding System Platform to System Manager.....	923
Adding Application type elements to System Manager.....	925
Adding Utility Services to System Manager.....	925
Adding a Communication Manager instance to System Manager.....	926
Adding a Session Manager instance to System Manager.....	927
Adding an Application Enablement Services instance to System Manager.....	928
Adding G430 or G450 Branch Gateway to System Manager.....	928
Adding an Avaya Messaging profile for a user.....	929
Product Initiated Registration overview.....	930
Configuring SAL Gateway.....	930
Configuring Avaya Services registration.....	931
Viewing notification status.....	932
Viewing certificate add status of elements.....	933
Field descriptions.....	933
Manage Elements field descriptions.....	933
Element details field descriptions.....	936
Delete Element Confirmation field descriptions.....	943
Import Elements field descriptions.....	944
Import Status field descriptions.....	946
Add Communication Manager field descriptions.....	947
Adding an Application Enablement Services instance to System Manager field descriptions.....	951
Add IP Office field descriptions.....	952
Delete IP Office field descriptions.....	954

Managing Serviceability Agents.....	954
Serviceability Agents.....	954
Converting a common alarm definition file to MIB file and trapd file.....	955
Configuration files in the MIBTOOL.jar file.....	955
generateTrapdAndMibUnix.....	956
Managing SNMPv3 user profiles.....	956
Managing SNMP target profiles.....	959
Notification filtering.....	962
Managing user and target profiles.....	967
Synchronization of Data.....	972
Communication Manager, Messaging data, and IP Office synchronization.....	972
Synchronizing the Communication Manager data and configuring options.....	974
Initializing synchronization.....	975
Initializing incremental synchronization.....	975
Synchronizing the IP Office system configuration.....	976
Synchronizing the UCM and Application Server system configuration.....	977
Synchronizing the VMPro system configuration.....	977
Synchronizing the messaging data.....	978
Saving the Communication Manager translations.....	978
About CM audit.....	979
Performing a Communication Manager audit.....	979
CM audit field descriptions.....	979
Audit report field descriptions.....	980
Communication Profiles synchronization.....	980
Communication profiles synchronization.....	980
Synchronizing the CS 1000 profile.....	981
Assigning anonymous profiles.....	982
Deleting anonymous profiles.....	982
Cleaning up communication profiles.....	983
Synchronize communication profiles field descriptions.....	983
Anonymous Communication Profiles field descriptions.....	984
Average duration of CS 1000 account operations.....	985
Connection pooling.....	985
Connection pooling.....	985
Configuring Communication Manager Connection Pool.....	985
Connection Pooling field descriptions.....	987
Modifying the maximum number of simultaneous logins for a user.....	988
Configure options.....	988
Chapter 14: Managing events.....	990
Managing alarms.....	990
Alarming.....	990
Cluster level alarming.....	990
Remote key server alarms.....	991

Viewing alarms.....	991
Changing the alarm status.....	991
Exporting alarms.....	992
Deleting alarms.....	992
Filtering alarms.....	992
Searching for alarms.....	993
Changing the throttle period from default 720 minutes to other period for specific alarm	994
Generating test alarms.....	994
Managing Geographic Redundancy related alarms.....	996
AutoRefresh Alarm List field descriptions.....	997
Alarming field descriptions.....	999
Managing logs.....	1002
Logging service.....	1002
Log Types.....	1003
Managing log harvester.....	1004
Managing log settings.....	1017
Managing log viewer.....	1023
Audit Logging.....	1029
TrapListener service.....	1030
Chapter 15: Managing licenses.....	1031
WebLM overview.....	1031
Obtaining the license file.....	1031
Finding LAC for System Manager in PLDS.....	1032
Accessing WebLM.....	1032
Installing a license file.....	1033
Client node locking.....	1034
Viewing the license capacity and utilization of the product features	1034
Viewing peak usage for a licensed product.....	1035
Uninstalling a license file.....	1035
Viewing the server properties.....	1036
WebLM Home field descriptions.....	1036
Install license field descriptions.....	1037
View License Capacity field descriptions.....	1037
View Peak Usage field descriptions.....	1038
Centralized licensing.....	1039
About centralized licensing.....	1039
Enabling centralized licensing.....	1040
Configure centralized licensing field descriptions.....	1040
Adding an element instance and assigning the element instance to a license file.....	1041
Editing an element instance and license file assignment.....	1042
Deleting an element instance.....	1043
Element instance field descriptions.....	1043
Disabling centralized licensing.....	1044

Uninstall license field descriptions.....	1044
Server Properties field descriptions.....	1045
Adopter application cannot communicate with WebLM Server.....	1045
Enterprise licensing	1046
Configuring enterprise licensing.....	1046
Retrieving the local WebLM certificate from browser.....	1047
Adding local WebLM certificate as trusted certificate in System Manager.....	1048
Adding a local WebLM server.....	1048
Modifying a local WebLM server configuration.....	1049
Removing a local WebLM server.....	1050
Viewing the license capacity of the licensed features of a product.....	1050
Viewing the connectivity status of the local WebLM servers	1051
Validating connectivity to local WebLM servers for a product.....	1051
Viewing usage by WebLM.....	1051
Viewing enterprise usage of a license feature.....	1052
Viewing the periodic status of the master and local WebLM servers.....	1052
Querying usage of feature licenses for master and local WebLM servers.....	1053
Changing allocations of licensed features for a local WebLM server.....	1053
Viewing allocations by features.....	1054
Viewing allocations by the local WebLM server.....	1054
Viewing usage summary.....	1054
View by feature field descriptions.....	1055
View by local WebLM field descriptions.....	1055
Enterprise Configuration field descriptions.....	1055
View Local WebLMs field descriptions.....	1057
Add local WebLM field descriptions.....	1058
Modify local WebLM field descriptions.....	1059
Delete local WebLM field descriptions.....	1061
Deletion of the local WebLM server.....	1061
Usage Summary field descriptions.....	1061
Usage by WebLM field descriptions.....	1062
Enterprise Usage field descriptions.....	1063
Query Usage field descriptions.....	1064
Allocations by Features field descriptions.....	1065
Allocations by Local WebLM field descriptions.....	1066
Change Allocations field descriptions.....	1066
Periodic Status field descriptions.....	1067
Metering Collector configuration overview.....	1068
Metering Collector Configuration field descriptions.....	1068
Deleting the metering collector configuration.....	1069
Chapter 16: Data Replication Service.....	1070
Data Replication Service.....	1070
Synchronization in a Geographic Redundancy scenario.....	1071

DRS client audit.....	1071
Viewing replica groups.....	1072
Viewing replica nodes in a replica group.....	1072
Repairing a replica node.....	1073
Repairing all replica nodes in a replica group.....	1073
Viewing replication details for a replica node.....	1074
Removing a replica node.....	1074
Removing a replica node from the queue.....	1074
Replica Groups field descriptions.....	1075
Replica Nodes field descriptions.....	1076
Replication Node Details field descriptions.....	1079
Chapter 17: Managing reports.....	1082
Reports.....	1082
Support for generating endpoint reports with buttons.....	1082
Reports Generation field descriptions.....	1083
Generating a detailed report.....	1084
Generating a basic report.....	1085
New Report field descriptions.....	1085
Editing report parameters.....	1088
Rerunning reports.....	1088
Customizing reports.....	1089
Downloading reports.....	1090
Reports History field descriptions.....	1091
Configuring email properties.....	1091
Sending reports through email.....	1092
Deleting reports.....	1092
Configuring report properties.....	1092
Remote server configuration.....	1093
Adding a remote server.....	1093
Viewing the details of a remote server.....	1093
Editing the details of a remote server.....	1094
Deleting a remote server.....	1094
Add Server field descriptions.....	1094
Remote Server Configuration field descriptions.....	1095
Chapter 18: Managing scheduled jobs.....	1096
Scheduler.....	1096
Functions of the User Management scheduled job.....	1097
Accessing scheduler.....	1097
Assigning permissions to access Scheduler.....	1097
Viewing pending jobs.....	1098
Viewing completed jobs.....	1099
Viewing logs for a job.....	1099
Filtering jobs.....	1099

Editing a job.....	1100
Deleting a job.....	1100
Disabling a job.....	1101
Enabling a job.....	1102
Stopping a job.....	1102
Pending Jobs field descriptions.....	1103
Completed Jobs field descriptions.....	1105
Job Scheduling-View Job field descriptions.....	1106
Job Scheduling-Edit Job field descriptions.....	1108
Job Scheduling-On Demand Job field descriptions.....	1109
Disable Confirmation field descriptions.....	1110
Stop Confirmation field descriptions.....	1111
Delete Confirmation field descriptions.....	1112
Chapter 19: Templates.....	1114
Template management.....	1114
Template versioning.....	1114
Filtering templates.....	1114
Upgrading a template.....	1115
Adding CM Agent template.....	1116
Editing CM Agent template.....	1116
Viewing CM Agent template.....	1117
Deleting CM Agent template.....	1117
Duplicating CM Agent template.....	1117
Adding CM Endpoint templates.....	1118
Editing CM Endpoint templates.....	1118
Viewing CM Endpoint templates.....	1119
Deleting CM Endpoint templates.....	1119
Duplicating CM Endpoint templates.....	1120
Assigning permissions for CM templates.....	1120
Adding subscriber templates.....	1121
Editing subscriber templates.....	1122
Viewing subscriber templates.....	1123
Deleting subscriber templates.....	1123
Duplicating subscriber templates.....	1123
Viewing associated subscribers.....	1124
Templates List.....	1124
Add Agent Template field descriptions.....	1126
Subscriber Messaging Templates field descriptions.....	1132
Subscriber CMM Templates field descriptions.....	1135
Subscriber MM Templates field descriptions.....	1137
Managing IP Office Endpoint template.....	1140
Adding an IP Office endpoint template.....	1140
Viewing an IP Office endpoint template.....	1141

Editing an IP Office endpoint template.....	1141
Duplicating an IP Office endpoint template.....	1142
Deleting an IP Office endpoint template.....	1142
Upgrading IP Office endpoint templates.....	1143
IP Office endpoint template field descriptions.....	1143
Managing IP Office System Configuration template.....	1144
Adding an IP Office System Configuration template.....	1144
Viewing an IP Office System Configuration template.....	1145
Editing an IP Office system configuration template.....	1145
Deleting an IP Office system configuration template.....	1146
Applying an IP Office system configuration template on an IP Office device.....	1146
IP Office System Configuration template field descriptions.....	1147
Manage audio files.....	1147
Uploading an audio file.....	1148
Converting a .WAV audio file to a .C11 audio file.....	1148
Deleting an audio file.....	1149
Manage Audio field descriptions.....	1149
Managing UCM and Application Server system configuration templates.....	1150
Adding a UCM and Application Server Configuration template.....	1150
Viewing a UCM and Application Server Configuration template.....	1151
Editing a UCM and Application Server Configuration template.....	1151
Deleting a UCM and Application Server Configuration template.....	1152
Applying a UCM and Application Server Configuration template.....	1153
UCM and Application Server Templates field descriptions.....	1154
Managing VMPro system configuration templates.....	1154
Adding a VMPro System Configuration template.....	1154
Viewing a VMPro System Configuration template.....	1155
Editing a VMPro System Configuration template.....	1155
Deleting a VMPro System Configuration template.....	1156
Applying a VMPro System Configuration template on a device.....	1156
Duplicating a VMPro System Configuration template.....	1157
VMPro System Configuration Templates field descriptions.....	1157
Managing VMPro call flow templates.....	1158
Adding a VMPro Call Flow template.....	1158
Viewing a VMPro Call Flow template.....	1158
Editing a VMPro Call Flow template.....	1159
Deleting a VMPro Call Flow template.....	1159
Applying a VMPro Call Flow template on a device.....	1160
Duplicating a VMPro Call Flow template.....	1161
VMPro Call Flow Templates field descriptions.....	1161
Chapter 20: Security.....	1162
Extended Security Hardening.....	1162
Enabling Commercial Grade Hardening.....	1163

Enabling Military Grade Hardening.....	1164
Optional settings for security hardening.....	1165
Security hardening options.....	1166
Enabling security hardening options.....	1166
Disabling security hardening options.....	1167
Viewing the status of the security hardening options.....	1167
Configuring the TLS cipher suite list.....	1168
Changing the TLS version.....	1168
Changing the TLS version of System Manager.....	1168
Changing the TLS version of primary and secondary System Manager.....	1169
outboundConnectionLogging command.....	1170
Enabling outbound connection logging.....	1170
Disabling outbound connection logging.....	1171
configureOutboundFirewall command.....	1171
Configuring the outbound firewall rules.....	1173
Viewing the list of outbound firewall rules.....	1174
Viewing the outbound firewall rule status.....	1174
Removing outbound firewall rules.....	1175
Disabling the outbound firewall rule.....	1175
Overwriting the existing outbound firewall rules.....	1176
Managing the outbound firewall rule logging.....	1177
Managing certificates.....	1178
Trust Management.....	1178
Certificate generation and certificate management capabilities in System Manager.....	1178
Setting the enrollment password.....	1181
Managing trusted certificates.....	1183
Managing identity certificates.....	1190
Certificate Revocation.....	1197
Manage Entity Classes.....	1200
manageEntityClassWhitelist command.....	1204
Retrieving the System Manager CA certificate.....	1209
Certificate Authorities.....	1209
Applying third-party certificates to Appliance Virtualization Platform.....	1210
Creating or editing generic CSR.....	1211
Generating certificates from System Manager.....	1212
External SSL configurations in System Manager.....	1223
Set the System Manager CA as the subordinate CA.....	1224
Configuring DTLS for CS 1000.....	1233
Configuring SIP TLS for CS 1000.....	1233
Managing certificate revocation list.....	1233
Deletion of expired certificates from System Manager.....	1238
Extended Hostname Validation.....	1239
Enabling Extended Hostname Validation.....	1239

External authentication.....	1239
External authentication.....	1239
Editing the authentication scheme.....	1240
Provisioning of authentication servers.....	1241
Provisioning the LDAP server.....	1241
Provisioning the RADIUS server.....	1242
Provisioning the Kerberos server.....	1242
Provisioning user certificate authentication.....	1243
Authentication Servers field descriptions.....	1243
SAML authentication.....	1245
Active sessions.....	1250
Viewing active sessions.....	1250
Terminating Single Sign-On sessions.....	1250
Regenerating data protection keys.....	1251
Regenerating symmetric keys for System Manager.....	1251
Regenerating asymmetric keys for System Manager.....	1252
Regenerating asymmetric keys for geographic redundancy-enabled System Manager.....	1252
Chapter 21: Managing tenants.....	1254
Multi Tenancy.....	1254
Enabling Multi Tenancy.....	1255
Creating a tenant.....	1256
Assigning the tenant administrator to the tenant.....	1259
Unassigning the tenant administrator.....	1260
Viewing the tenant.....	1260
Modifying the tenant.....	1261
Deleting a tenant.....	1261
Multi Tenancy for Avaya SIP AST endpoints.....	1263
Multi Tenancy for Communication Manager objects.....	1263
Notes on Multi Tenancy for Communication Manager.....	1264
Tenant Management field descriptions.....	1267
Create Tenant field descriptions.....	1267
Chapter 22: Shutting down System Manager.....	1272
Overview.....	1272
Shutting down System Manager from the web console.....	1273
Rebooting System Manager virtual machine from the web console.....	1274
Viewing the shutdown history from the System Manager web console.....	1274
Shutdown System Manager field descriptions.....	1275
Chapter 23: Solution deployment and upgrade.....	1276
Solution Deployment Manager.....	1276
Solution Deployment Manager overview.....	1276
Solution Deployment Manager Client.....	1277
Solution Deployment Manager.....	1285
Solution Deployment Manager configuration settings	1287

User settings.....	1287
Establishing PLDS connection to Avaya.....	1287
Establishing the connection to an alternate source.....	1288
User Settings field descriptions.....	1291
Software library management.....	1292
Software library.....	1292
Enabling and disabling FTP on System Manager.....	1293
Configuring System Manager as local software library.....	1294
Configuring external server as a remote software library for upgrades.....	1294
Creating a software library.....	1303
Editing a software library.....	1304
Viewing a software library.....	1304
Deleting a software library.....	1304
Software library field descriptions.....	1305
Viewing a file in the software library.....	1307
Downloading the OVA file to System Manager.....	1307
Uploading a file to the software library.....	1308
Deleting a file from the software library.....	1309
Software Library Files field descriptions.....	1309
System requirements for the external server.....	1310
Applications pre-upgrade functions.....	1311
Refreshing elements.....	1311
Analyzing software.....	1311
Downloading the software.....	1312
File Download Manager field descriptions.....	1313
Performing the preupgrade check.....	1314
Preupgrade Configuration field descriptions.....	1315
Application management.....	1316
Application management.....	1316
Managing the location.....	1317
Managing the platform.....	1319
Certificate validation.....	1347
Managing the application.....	1351
Monitoring a host and virtual machine.....	1377
Managing vCenter.....	1377
Managing syslog profiles.....	1383
Viewing the job history of virtual machine operations.....	1386
Application Management field descriptions.....	1386
Job History field descriptions.....	1391
Upgrading Avaya Aura® applications.....	1392
Upgrade Management overview.....	1392
Avaya Aura® applications upgrade.....	1393
Upgrade checklist for Avaya Aura® Virtual Appliance	1394

Upgrade target release selection.....	1396
Installing software patches by using Solution Deployment Manager.....	1397
Installing custom software patches.....	1399
Installed Patches field descriptions.....	1401
Upgrade Management field descriptions.....	1402
Upgrade Configuration field descriptions.....	1404
Edit Upgrade Configuration field descriptions.....	1405
Uploading a custom patch.....	1413
Uploading custom patch field descriptions.....	1413
Migrating System Platform-based elements or bare metal-based Communication Manager elements.....	1414
Upgrading Branch Session Manager instances in bulk.....	1422
System Manager upgrade management.....	1426
Upgrade Management field descriptions.....	1426
Add Element field descriptions.....	1427
Edit Elements field descriptions.....	1428
Upgrade Management field descriptions.....	1428
Upgrade job status.....	1436
Upgrade job status.....	1436
Viewing the Upgrade job status.....	1437
Editing an upgrade job.....	1437
Deleting the Upgrade jobs.....	1437
Upgrade Job Status field descriptions.....	1438
Upgrades to Communication Manager Release 6.3.100.....	1439
Communication Manager upgrades.....	1439
Checklist for upgrading Communication Manager to Release 6.3.100.....	1440
Getting inventory.....	1443
Analyze software.....	1444
Analyzing the software.....	1445
Downloading the software.....	1445
Performing a preupgrade check.....	1446
Preupgrade checks.....	1448
Preupgrade checklist for Linux [®] Operating System upgrades.....	1449
Pre-upgrade checklist for System Platform upgrades.....	1449
Hardware requirement checks during a preupgrade check.....	1450
Preupgrade status	1451
Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.....	1451
Upgrading Communication Manager 5.2.1.....	1463
Server support for Communication Manager Release 5.2.1 to 6.3.100 upgrades.....	1476
Upgrading TN boards.....	1478
Upgrading media gateways and media modules.....	1478
G430 Branch Gateway and G450 Branch Gateway multistep upgrade overview.....	1480
Downloading a file.....	1483

Upgrading Communication Manager 5.x.....	1484
Upgrading Communication Manager 5.x.....	1484
Updating Communication Manager.....	1485
Updating the SAMP/MPC firmware.....	1486
Protocol matrix for upgrades.....	1486
Uploading the version.xml file.....	1487
Chapter 24: Data Encryption.....	1489
Remote Key Server.....	1490
Data Encryption password policy.....	1490
Data encryption commands.....	1491
encryptionPassphrase command.....	1491
encryptionRemoteKey command.....	1493
encryptionLocalKey command.....	1495
Viewing data encryption status.....	1496
Chapter 25: Communication Manager Notify Sync.....	1497
Communication Manager notify synchronization.....	1497
Downloading the System Manager PEM certificate.....	1498
Downloading the pem file to Communication Manager.....	1499
Adding a trusted certificate to Communication Manager.....	1500
Configuring notify sync between Communication Manager and System Manager.....	1501
Configure two-way TLS.....	1503
Adding the Communication Manager certificate to the System Manager trust.....	1503
Enabling two-way TLS in System Manager.....	1504
Chapter 26: System Manager Network Configuration.....	1505
Out of Band Management in System Manager.....	1505
Configuring Out of Band Management on System Manager.....	1506
Configuring Out of Band Management on System Manager in the Geographic Redundancy setup.....	1507
Changing the IP address and FQDN in System Manager.....	1508
Impact of change in FQDN and IP address on the Geographic Redundancy feature.....	1508
SSO login to remote machine fails.....	1509
Changing network parameters on System Manager.....	1509
Changing IP address or FQDN of managed elements.....	1512
Changing the System Manager IP address in managed elements.....	1512
Changing the IP address and FQDN on the System Manager servers in Geographic Redundancy.....	1513
Change in IP address and FQDN on the primary and secondary System Manager servers	1513
Changing the IP address and FQDN on the primary System Manager when the secondary is in the standby or active mode.....	1513
Changing the IP address and FQDN on the primary System Manager server when the secondary is nonoperational.....	1514
Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode.....	1515

Changing the IP address and FQDN on the secondary System Manager server when the primary is nonoperational.....	1516
System Manager command line interface operations.....	1518
Chapter 27: Configuring the date and time.....	1529
Verifying changes to the date and time configuration.....	1529
Configuring System Manager logs for Syslog server.....	1529
Changing date and time on System Manager running on VMware.....	1530
Configuring the NTP server.....	1530
Configuring the time zone.....	1530
Chapter 28: System Manager localization.....	1531
Installing language pack on System Manager.....	1532
Chapter 29: Resources.....	1533
System Manager documentation.....	1533
Finding documents on the Avaya Support website.....	1534
Accessing the port matrix document.....	1534
Avaya Documentation Center navigation.....	1535
Training.....	1536
Viewing Avaya Mentor videos.....	1536
Support.....	1537
Using the Avaya InSite Knowledge Base.....	1537
Appendix A: Firewall implementation in System Manager.....	1539
Firewall basics.....	1539
Firewall implementation in System Manager.....	1539
Appendix B: Communication Manager reports available through System Manager...	1541
List reports.....	1541
Display reports.....	1551
Status reports.....	1556
Appendix C: Remote Access.....	1560
Remote access of System Manager.....	1560
EASG login for System Manager.....	1560
Logging on to the System Manager web console by using EASG login.....	1561

Chapter 1: Introduction

Purpose

This document provides procedures for configuring Avaya Aura® System Manager and the Avaya Aura® applications and systems that System Manager manages.

The primary audience for this document is anyone who is involved with configuring, troubleshooting, maintaining and verifying System Manager at a customer site. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Change history

The following changes are made to this document since the last issue:

Issue	Date	Summary of changes
10	March 2021	Updated the following sections: • Generating the communication profile password from the self provisioning interface on page 222 • User Profile Add field descriptions on page 295 • Synchronize CM Data and Configure Options / Element Cut-Through field descriptions on page 709 • Configuration of IP Phone Group ID on SIP Devices on page 747

Table continues...

Issue	Date	Summary of changes
9	February 2021	For Release 8.1.3.1, added the section: New in System Manager Release 8.1.3.1 on page 38 For Release 8.1.3.1, updated the following sections: • System Manager web console on page 46 • System Manager Dashboard field descriptions on page 48 • System Manager message with login details on page 50 • System Manager alert messages at login on page 51 • Directory synchronization overview on page 80
8	November 2020	Updated the section: New in System Manager Release 8.1.3 on page 39

Table continues...

Issue	Date	Summary of changes
7	October 2020	For Release 8.1.3, added the following sections: • New in System Manager Release 8.1.3 on page 39 • System Manager message with login details on page 50 • setSecurityPolicy command on page 64 • Managing the password policies through CLI on page 65 • Changing the password policies through CLI on page 66 • Viewing the password policy status on page 68 • Displaying the password policies on page 69 • Restoring the default password policy settings on page 69 • Refreshing the default password policy settings on page 70 • Migration of J1xx endpoints configured as 96x1 SIP set type on page 725 • Criteria for migrating 96x1 SIP set type to J1xx set type on page 725 • Enabling the Discover Endpoint eligible for migration job on page 727 • Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search on page 727 • Migrating set type of selected J1xx endpoint from 96x1 SIP to J1xx set type on page 728 • Migrating set type of all J1xx endpoint from 96x1 SIP to J1xx set type on page 730 • Viewing endpoint migration job history on page 731 • Cancelling an endpoint migration job on page 732 • Deleting endpoint migration job on page 733 • Endpoint Migration field descriptions on page 733 • Endpoint Migration Job History field descriptions on page 734 • outboundConnectionLogging command on page 1170 • Enabling outbound connection logging on page 1170 • Disabling outbound connection logging on page 1171 • configureOutboundFirewall command on page 1171 • Configuring the outbound firewall rules on page 1173 • Viewing the list of outbound firewall rules on page 1174 • Viewing the outbound firewall rule status on page 1174 • Removing outbound firewall rules on page 1175 • Disabling the outbound firewall rule on page 1175

Table continues...

Issue	Date	Summary of changes
		• Overwriting the existing outbound firewall rules on page 1176 • Managing the outbound firewall rule logging on page 1177 • Manage Entity Classes on page 1200 • Adding an entity class on page 1200 • Editing an entity class on page 1201 • Deleting an entity class on page 1201 • Filtering entity classes on page 1201 • Manage Entity Classes field descriptions on page 1202 • Add Entity Class Update Entity Class field descriptions on page 1203 • manageEntityClassWhitelist command on page 1204 • Adding subject names for an entity class on page 1206 • Displaying subject names for an entity class on page 1207 • Viewing the subject name for an entity class on page 1207 • Viewing the subject name validation status for an entity class on page 1208 • Deleting the subject names for an entity class on page 1208 • Deletion of expired certificates from System Manager on page 1238 • Rebooting System Manager virtual machine from the web console on page 1274 • Viewing the shutdown history from the System Manager web console on page 1274 • Shutdown System Manager field descriptions on page 1275 For Release 8.1.3, updated the following sections: • Logging on to the System Manager web console on page 49 • System Manager alert messages at login on page 51 • Password strength policy enforcement on page 60 • Password history policy enforcement on page 60 • Password policies field descriptions on page 61 • User synchronization datasource field descriptions on page 85 • User Profile Add field descriptions on page 295 • Communication profile password policy on page 609 • Communication Profile Password Policy field descriptions on page 611 • View and Edit Profile SMGR field descriptions on page 874 • View Profile: TrustManagement field descriptions on page 890

Table continues...

Issue	Date	Summary of changes
		• Edit Profile: TrustManagement field descriptions on page 891 • View Profile: Communication System Management Configuration field descriptions on page 866 • Edit Profile: Communication System Management Configuration field descriptions on page 867 • Shutting down System Manager from the web console on page 1273 • Authentication Servers field descriptions on page 1243 • Create AVP Kickstart field descriptions on page 1329 • Generating and accepting the Appliance Virtualization Platform host certificates on page 1348 • New vCenter and Edit vCenter field descriptions on page 1381
6	April 2020	Added the following sections: • User searchable fields on page 248 • Searching for users by using Search component on page 249 • System Manager localization on page 1531 Updated the following sections: • System Manager web console on page 46 • Restoring the backup through the command line interface on page 849 • Upgrade Management overview on page 1392 • Installing language pack on System Manager on page 1532

Table continues...

Issue	Date	Summary of changes
5	March 2020	For Release 8.1.2, added the following sections: • New in System Manager Release 8.1.2 on page 41 • Excluded log files on page 859 • Applying data retention rule on page 861 • logRetention command on page 862 • updateLogRetention command on page 863 • pruneAllLogs command on page 863 • Remote key server alarms on page 991 • Data Encryption on page 1489 • Remote Key Server on page 1490 • Data Encryption password policy on page 1490 • encryptionPassphrase command on page 1491 • Adding encryption passphrase on page 1491 • Changing encryption passphrase on page 1491 • Removing encryption passphrase on page 1492 • Displaying encryption passphrase and slot assignment on page 1492 • encryptionRemoteKey command on page 1493 • Adding remote key server on page 1493 • Removing remote key server on page 1494 • Displaying remote key server and slot assignment on page 1494 • encryptionLocalKey command on page 1495 • Enabling local key store on page 1495 • Disabling local key store on page 1495 • Viewing data encryption status on page 1496 For Release 8.1.2, updated the following sections: • Agents field descriptions on page 663 • Enabling backup encryption on page 842 • Creating a data backup on a local server on page 842 • Creating a data backup on a remote server on page 843 • Restoring data backup from a local server on page 847 • Restoring a backup from a remote server on page 848 • Backup field descriptions on page 853

Table continues...

Issue	Date	Summary of changes
		• Restore field descriptions on page 856 • Data retention rules on page 859 • Data Retention field descriptions on page 862 • Edit Logger field descriptions on page 1020 • Edit Appender field descriptions on page 1021
4	October 2019	For Release 8.1.1, added the following sections: • New in System Manager Release 8.1.1 on page 41 • Holiday Table List on page 686 • Exporting all Holiday Table on page 686 • Exporting selected holiday table on page 687 • Importing holiday table on page 687 • Downloading Excel Template on page 688 • Service Hours Table List on page 695 • Exporting all Service Hours Table on page 696 • Exporting selected service hours table on page 696 • Importing service hours table on page 696 • Downloading Excel Template on page 697 • Configuration of IP Phone Group ID on SIP Devices on page 747 • Configuring the IP Phone Group ID for an endpoint on page 748 • Phone view layout of SIP Endpoints on page 757 • Endpoint display mode on page 759 • Support of common parameter across endpoint template on page 765 • VM Console overview on page 1361 • Opening a VM console from Solution Deployment Manager on page 1362 • VM Console field descriptions on page 1363 For Release 8.1.1, updated the following sections: • New User Provisioning Rule field descriptions on page 619 • IP Phone Group ID on page 747 • Button Assignment on page 756 • Broadcasting announcements on page 676

Table continues...

Issue	Date	Summary of changes
3	July 2019	Updated the following sections: • Geographic Redundancy prerequisites overview on page 105 • Disaster recovery prerequisites on page 124 • View and Edit Profile Messaging field descriptions on page 871 • Adding an Avaya Messaging profile for a user on page 929
2	June 2019	Added the Accessing the port matrix document on page 1534 section. Updated the Hardware resource and parameter for the Geographic Redundancy setup on page 101 section.
1	June 2019	Release 8.1 document.

Chapter 2: Overview

System Manager overview

System Manager is a central management system that delivers a set of shared management services and provides a common console for the Avaya Aura® applications and systems.

System Manager includes the following shared management services:

Service	Description
Solution Deployment Manager	To: • Deploy Avaya Aura® applications. • Upgrade and migrate Avaya Aura® applications.  Note: When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application. For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website. • Download Avaya Aura® applications. • Install service packs, feature packs, and software patches for the following Avaya Aura® applications: - Communication Manager and associated devices, such as gateways, media modules, and TN boards. - Session Manager - Branch Session Manager - AVP Utilities - Avaya Aura® Appliance Virtualization Platform, the ESXi host that is running on the Avaya Aura® Virtualized Appliance. With the Solution Deployment Manager client, you can: • Deploy Avaya Aura® applications • Upgrade System Manager • Install software patches for System Manager

Table continues...

Service	Description
Users	Provides features to administer users, shared address, public contact list, and information of system presence access control list. You can: • Associate the user profiles with groups, roles, and communication profiles • Create a contact list • Add an address and private contacts for the user
User Provisioning Rules	To create user provisioning rules. When the administrator creates the user with the user provisioning rule, the system populates the user attributes from the rule. The administrator requires to provide minimal information.
Bulk import and export	To provide bulk import and export of user profiles and global settings.
Directory synchronization	To provide bidirectional synchronization of user attributes from System Manager to the LDAP directory server.
Elements	To provide features of individual components of System Manager. Some links provide access to generic features of System Manager. Most links provide access to features provided by System Manager components.
Events	To administer alarms and logs generated by System Manager and other components of System Manager. Serviceability agent sends alarms and logs to SAL Gateway and System Manager, which in turn forwards the alarms and logs to the Avaya Data Center. You can view and change the status of alarms. You can view logs and harvest logs for System Manager and the components, and manage loggers and appender.
Geographic Redundancy	To handle scenarios when the primary System Manager server fails or the data network fragments. In such a scenario, the system manages and administers elements such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the customer enterprise using the secondary System Manager server.
Groups and Roles	To administer groups and roles. You can create and manage groups, roles, and permissions.
Licenses	To administer licenses for individual components of Avaya Aura® Unified Communication System.
Security	To: • Authenticate using certificates • Configure the certificate authority

Table continues...

Service	Description
System Manager data	To: • Back up and restore System Manager configuration data • Monitor and schedule jobs • Replicate data from remote nodes • Configure data retention settings and profiles for various services that System Manager provides
Tenant Management	To: • Create a tenant • Edit tenant details • Duplicate an existing tenant • Delete a tenant

New in this release

New in System Manager Release 8.1.3.1

Avaya Aura® System Manager Release 8.1.3.1 supports the following new feature and enhancements:

Support for Active Directory 2019

With Release 8.1.3.1, System Manager supports Active Directory 2019.

Removal of the System Manager message pop-up with last login details

From Release 8.1.3.1, System Manager does not display the message pop-up window at login.

The last login information is now displayed in the **Notifications** widget on the System Manager dashboard.

Enhancements to the System Manager Alert messages at login

From Release 8.1.3.1, System Manager does not display the Session Manager emergency Dial Pattern routes notification message for Emergency Location Management Solution in an Alert Message pop-up window.

The emergency Dial Pattern routes notification message is now displayed in the **Notifications** widget on the System Manager dashboard.

Enhancements to the Notifications widget

From Release 8.1.3.1, the **Notifications** widget on the System Manager dashboard also displays the user login information and emergency Dial Pattern routes notification message for Emergency Location Management Solution.

From System Manager Release 8.1.3.1 and later, you cannot close the **Notifications** widget.

New in System Manager Release 8.1.3

Avaya Aura® System Manager Release 8.1.3 supports the following new features and enhancements:

Migration of 96x1 endpoints to J-Series phone

With Release 8.1.3, System Manager supports the migration of 96x1 endpoints to the J-Series phone. For migration of endpoints, System Manager and Session Manager must be on Release 8.1.3 or later.

Service observe support for J-Series endpoints

With Release 8.1.3, Communication Manager and System Manager supports the **sip-sobsrv** button for the following J-Series endpoints: J169 and J179.

Support of apostrophe character for Login Name

With Release 8.1.3, the **Login Name** field on the **Users > User Management > Manage Users** page, supports login names with an apostrophe ('). This helps import a user that has a login name with an apostrophe.

Support of 256-character password length for LDAP Server credentials

With Release 8.1.3, System Manager supports a 256-character password. Configure the password in one of the following ways:

- On the **Users > Administrators > User Services > External Authentication** page in the **Password for Root Binding** field.
- On the **Users > Directory Synchronization > Sync Users > User Synchronization** page, in the **Synchronization Datasources** tab when performing a New or Edit operation. On the New/Edit User Synchronization Datasource page in the **Password** field.

Simple Certificate Enrollment Protocol enhancement to improve Certificate Management for endpoints

With System Manager Release 8.1.3 and later, supports the following:

- Endpoints that have certificates issued by System Manager can use entity classes to send certificate enrollment or renewal requests to System Manager. You can add, edit, and delete entity classes using the **Services > Security > Certificates > Manage Entity Classes** page. You can manage the password for entity classes on the View Profile: SMGR page in the Password Policy for Programmatic Accounts section.
- You can add, list, view, and delete subject names for the provided entity class using the **manageEntityClassWhitelist** command. You can add and delete bulk entries of subject names for an entity class. You can also check the status of the subject name validation for the entity class.
- You can use the **Number of days after which system deletes expired certificates** field on the **Services > Configurations > Settings > SMGR > Trust Management** page to set the number of days to delete the expired certificates from the system.

Support for outbound connection logging

With Release 8.1.3, you can log all outgoing connections from System Manager, using the `outboundConnectionLogging` utility.

Support for configuring the outbound firewall rule

With Release 8.1.3, you can configure System Manager outbound firewall rule by using the `configureOutboundFirewall` utility. You can add, list, view status, disable, remove, and overwrite the IP addresses and FQDN in the whitelist for establishing the outbound connection from System Manager.

Support of new CLI command for managing the password policies

With Release 8.1.3, System Manager supports the `setSecurityPolicy` command for managing password policies using the command line interface (CLI). This command is only applicable for changing or setting up the password for a CLI user or a root user that you create at the time of deployment.

Enhancement to password policies

With Release 8.1.3, the Communication Profile Password Policy and the Password strength policy are enhanced with the following:

- **Minimum total length** supports the default value of 14 characters as the minimum number of characters that you must use in a password.
- **Previous passwords blocked** supports the default value of 10 for the number of latest passwords that the system maintains in its history.
- Supports the addition of the new **Maximum repeated consecutive characters** field.
- Supports the addition of the new **Maximum consecutive characters from same character type** field.

Support for VMware ESXi 7.0

With Release 8.1.3, Avaya Aura® applications support the VMware® vSphere ESXi 7.0 and VMware® vCenter Server 7.0 in the VMware virtualized environment.

System Manager Welcome message

From System Manager Release 8.1.3, after your first successful login, when you log in to the System Manager web console or the System Manager command line interface again, System Manager displays the Welcome <SystemManager_UserName> pop-up window at your each subsequent login.

Enhancements to the System Manager alert messages at login

With Release 8.1.3, for the Emergency Location Management Solution, System Manager displays the Session Manager emergency Dial Pattern routes notification warning message in an Alert Messages pop-up window, if the Routing Locations, Routing Policies, and Dial Patterns are not configured on Session Manager according to the emergency calling guideline.

Centralized subscription licensing

With Release 8.1.3, WebLM supports the Centralized subscription licensing feature for solution licenses.

Enhancement to the number of IP Office branches support

With Release 8.1.3, System Manager supports up to:

- 2000 IP Office branches with System Manager Profile 3.
- 3500 IP Office branches with System Manager Profile 4.

New in System Manager Release 8.1.2

Avaya Aura® System Manager Release 8.1.2 supports the following new features and enhancements:

Data Encryption

With Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized environments. Once you deploy the application with data encryption, you cannot disable data encryption after deployment and vice-versa.

Support for encrypted backup and restore

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

Support for log file retention period management

With Release 8.1.2, you can configure the automated purging rule for log files based on the retention period configured on the Data Retention page of System Manager web console. Default value for number of days to retain log files are 30 days.

Support for the Avaya Subscription license

With Release 8.1.2, WebLM supports the Avaya Subscription license. You can view the license usage of the Avaya Subscription license as **Metered**.

New in System Manager Release 8.1.1

Avaya Aura® System Manager Release 8.1.1 supports the following new features and enhancements:

VMware console for applications

With Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab for the application that reside on Appliance Virtualization Platform Release 7.1.2 and later.

Based on the role of the user, you can assign the permissions for accessing the console.

Support for deploying Avaya SBCE using Solution Deployment Manager

With Release 8.1.1, you can:

- Download the Avaya Session Border Controller for Enterprise (Avaya SBCE) OVA from the Download Management page.

- Deploy the Avaya SBCE OVA.

To support this System Manager must be deployed on Profile 3 and higher systems.

Busy indicator support for J-Series endpoints

With Release 8.1.1, System Manager supports the **busy-ind** button for the following J-Series endpoints: J169, J169CC, J179, J179CC.

Support for the IP Phone Group Id field for SIP endpoints

With Release 8.1.1, System Manager supports the **IP Phone Group Id** field on the **Feature Options** tab for SIP endpoints.

On Communication Manager, this field is available on the page 3 of the **add station** or **change station** command. With Release 8.1.1, **IP Phone Group Id** also supports SIP endpoints.

Support for read only phone view layout for SIP Endpoints

With Release 8.1.1, you can view the Read only phone view layout for SIP Endpoints.

Support for common parameter across endpoint template

With Release 8.1.1, when you create a SIP endpoint, the system retains the common parameter information so that when you login SIP endpoints of that same type or of another type, all your SIP Endpoints are able to retrieve and update any of the common parameters they utilize.

The common parameters are on the **Elements > Communication Manager > Endpoints > Manage Endpoints** page on the **Profile Settings** and **Button Assignment** tabs.

Bulk import and export of Holiday Table and Service Hours Tables

Bulk import and export of **Holiday Table** and **Service Hours Tables** using System Manager web console. For adding, deleting and updating Holiday Table and Service Hours Tables in bulk, you can download a pre-loaded excel <Excel template file name>.xlsx file from **More Actions > Download Excel Template** on the following pages:

- **Elements > Communication Manager > Call Center > Holiday Table**
- **Elements > Communication Manager > Call Center > Service Hours Tables**

Multiple audio files upload in single click for broadcasting announcement

With Release 8.1.1, you can upload more than one audio files (.wav) in single click by using the **Browse** option of the **Select Announcement File** field.

New in System Manager Release 8.1

Avaya Aura® System Manager Release 8.1 supports the following new features and enhancements:

Support for System Manager Profile 4

With Release 8.1, System Manager supports a new Profile 4. The Profile 4 supports 35000 to 300000 users with up to 5000 Branch Session Manager instances and 28 Session Manager instances with a single System Manager system in an Avaya Aura® deployment.

System Manager Profile 1 not supported

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.

Appliance Virtualization Platform Hypervisor

With Release 8.1, Appliance Virtualization Platform is based on the customized OEM version of VMware® ESXi 6.5.

Support for Red Hat Enterprise Linux operating system 7.6

With Release 8.1, you can deploy and upgrade Avaya Aura® applications on the Red Hat Enterprise Linux operating system 7.6.

Support of Windows Server 2016 for installing the Solution Deployment Manager client

With Release 8.1, you can install the Solution Deployment Manager client on the Windows Server 2016, 64-bit operating system.

Solution Deployment Manager enhancements

- Increased capacity for **Refresh, Analyze, Update/Upgrade** operations on multiple elements at the same time for System Manager:
 - Profile 2: 20 elements
 - Profile 3: 30 elements
 - Profile 4: 50 elements
- The `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet on the **Solution Deployment Manager > Upgrade Management > Download > Bulk Import Spreadsheet** page supports bulk upgrade of Branch Session Managers.
- During OVA deployment, the Network Parameters page is revamped to display wider UI elements to enhance user experience.

Appliance Virtualization Platform enhancements

On the **Solution Deployment Manager > Application Management > Platforms** tab, a new:

- **More Actions > AVP Firewall Rules** option is added to view Appliance Virtualization Platform firewall rules.
- **Advanced Configuration** tab is added on the **Change Network params > Change Network Settings > Host Network/IP Settings** page from where you can delete unused Port Groups that are not associated with any virtual machine.

Support for bulk upgrade of Branch Session Manager instances

With Release 8.1, you can perform bulk upgrade of Branch Session Manager instances by using the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet on the **Solution Deployment Manager > Upgrade Management > Download > Bulk Import Spreadsheet** page.

Remote Syslog profile enhancement

With Release 8.1, the Add Syslog Receiver page provides the following TLS authentication options when the **tcp** protocol is selected.

- **Server certificate authentication**
- **Mutual TLS authentication**

Support for managing Syslog receiver certificates for Remote Syslog receiver

With Release 8.1, you can:

- Add trusted certificates for Remote Syslog receiver by selecting the **SYSLOG** store type on System Manager.
- Create identity certificate to use with Remote Syslog receiver by selecting the *syslog* service name on System Manager.

Administration and Serviceability enhancements

- Serviceability Agents management supports background execution job for pushing SNMP Target/User Profiles to multiple Serviceability Agents.
- Manage Elements displays a progress bar indication of background notification operations for Geographic Redundancy state change operations.
- API based management operations off-loaded from Port 443 to new Port 10443.
- Data Replication Service supports 250 node repairs at a time for System Manager Profile 4.
- Typeahead support is provided for the:
 - **Host Name** field on **Services > Events > Log Harvester > Create New Profile**.
 - **Survivability Server** field on **Users > User Provisioning Rule > Communication Profile > Session Manager Profile**.
- Advanced Search feature is added on the following pages:
 - **Inventory > Manage Elements**
 - **Inventory > Manage Serviceability Agents > Serviceability Agent**
 - **Replication > Replica Groups > Replica Nodes**
- Automated purging rule is added in Data Retention for Aged Scheduler Completed Jobs.
- Adding certificates for more than one element of same type and same version creates background job for execution. You can view this on the Certificate Management Jobs page using **Inventory > Manage Elements > More Actions > View Certificate Add Status** on System Manager.

Crisis Alert support for SIP endpoints

With Release 8.1, Crisis Alert (**crss-alert**) button support is added for SIP phones. When an emergency call is initiated by an enterprise user, then the crisis-alert watcher's endpoint displays an alert including information about emergency call.

No Hold Conference for SIP endpoints

With Release 8.1, No hold conference (**no-hld-cnfr**) button support is added for SIP phones. No Hold Conference is the ability to add a party in conference without putting existing users on Hold.

EC500 button support for SIP endpoints

With Release 8.1, System Manager supports the **EC500** button for the following endpoints: 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, J169CC, J179CC, CS1K-IPCC (Avaya Device Adapter).

Call appearance and Bridged appearance with per button ring control for SIP endpoints

With Release 8.1, System Manager supports Call appearance (Abbreviated/Delayed ringing) and Bridged appearance with per button ring control for the following endpoints: 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, J169CC, J179CC, CS1K-IPCC (Avaya Device Adapter).

Enhancements to the 16-digit extension

With Release 8.1, Avaya Aura® applications extend support for configuration of 16-digit extension to the following Communication Manager objects.

- hunt groups

 Note:

Administration of hunt group with 16-digit group extension and group members.

- coverage answer groups
- ELIN
- abbr dial buttons
- Listed Directory Number

Supported browsers

Following are the minimum supported versions of the supported browsers:

- Internet Explorer 11
- Mozilla Firefox 65, 66, and 67

IP Office integration with System Manager

From Release 8.1, you can add and administer the IP Office element from the System Manager web console.

Log on to System Manager

Turning off the compatibility mode

About this task

You might not be able to view the status of some operations on the webpages using Microsoft Internet Explorer because Internet Explorer imposes a time-out limit for the server to return the data. To correct this problem, you must install the patch for Internet Explorer from the Microsoft website at <http://support.microsoft.com/kb/181050%20>.

If the compatibility mode is turned on, some System Manager features might not work in Internet Explorer version 8 onwards. Therefore, you must turn off the compatibility mode.

Procedure

1. On the menu, click **Tools > Compatibility View Setting**.
2. In the Compatibility View Settings dialog box, clear all check boxes.
3. Ensure that the **Websites you've added to Compatibility View** field does not contain the address of the System Manager website.

System Manager web console

System Manager provides a centralized access to all Avaya Aura® elements through a browser-based Avaya management console with a Single Sign-on.

* Note:

- On a client, a single sign-on workflow must have the same domain name as System Manager. The domain name of the System Manager server must match that of the web client server. For instance, if the hostname of System Manager is `smgr.ca.avaya.com`, the server with the web client can have a hostname such as `client.ca.avaya.com` or `client.us.avaya.com`.
- System Manager allows you to open seven tabs simultaneously. The default number of tabs allowed to open is five. However, you can set the value to the maximum of seven on the System Manager Web Console. The pages that are opened in each tab should be from different Element Managers. If you open pages falling under the same Element Manager, you may encounter an error based on the operation you are performing. For example, editing the same station in two tabs may throw an error message.

The resolution of the System Manager web console is 1024×768. The System Manager web console provides the following:

- Corporate logo: You can add a logo on the web console.
- **Options** icon (

All the operational links are available under different menus, such as, **Users**, **Elements**, **Services**, **Widgets**, and **Shortcuts**.

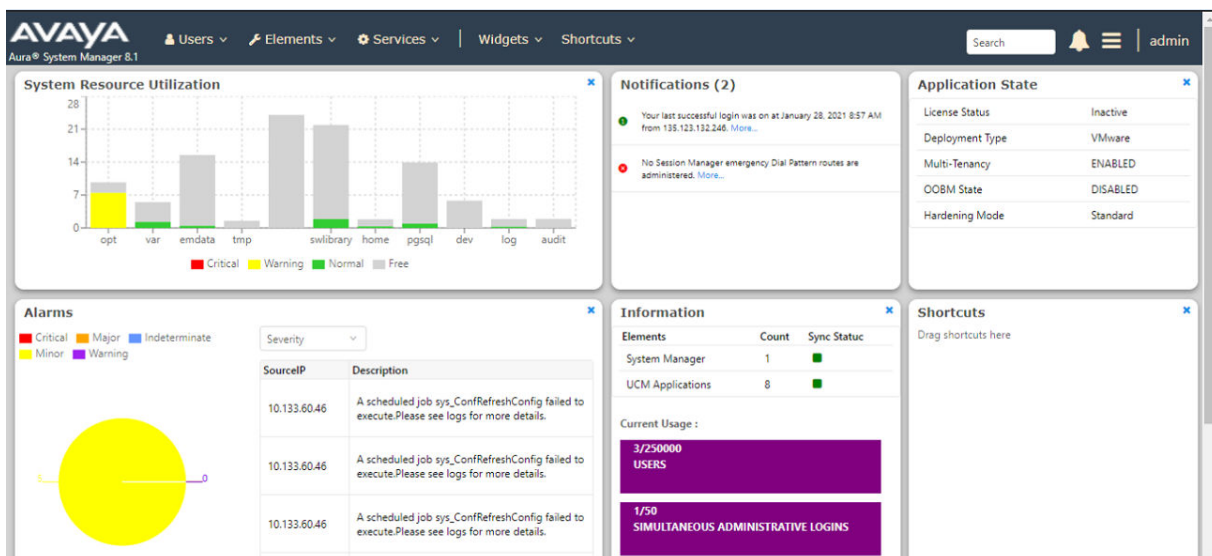
By default, the System Manager dashboard displays the following widgets:

- **Alarms**
- **Application State**
- **Notifications**
- **System Resource Utilization**
- **Information**
- **Shortcuts**

*** Note:**

After login, if you remove one of the default widgets, then it is available under the **Widgets** menu.

From System Manager Release 8.1.3.1 and later, you cannot close the **Notifications** widget. If you closed the **Notifications** widget during the last login on the System Manager Release 8.1.3 and earlier, then after upgrading to System Manager Release 8.1.3.1 and later, the system displays the default dashboard layout.



System Manager Dashboard field descriptions

Name	Description
System Resource Utilization	The resource utilization of the System Manager system in percentage (%). Displays the data of the directories, such as opt, var, emdata, tmp, perfddata, swlibrary, home, and pgsq. The following are the system resource utilization status: •  Critical •  Warning •  Normal •  Free
Notifications	The current notification from the application. From Release 8.1.3.1, the Notifications widget on the System Manager dashboard also displays the user login information and emergency Dial Pattern routes notification message for Emergency Location Management Solution. The messages in the Notifications widget are short. To view the additional details for each message, you can hover on the message. From System Manager Release 8.1.3.1 and later, you cannot close the Notifications widget. If you closed the Notifications widget during the last login on the System Manager Release 8.1.3 and earlier, then after upgrading to System Manager Release 8.1.3.1 and later, the system displays the default dashboard layout.
Shortcuts	The shortcut of the menu options.

Table continues...

Name	Description
Alarms	The alarms data of the application. You can sort the alarms by Severity, Age, and Element Type. The following are the alarm status based on Severity: •  Critical : Displays the number of critical alarms for the system. •  Major : Displays the number of major alarms for the system. •  Indeterminate : Displays the number of uncategorized alarms. •  Minor : Displays the number of minor alarms for the system. •  Warning : Displays the number of warning alarms for the system. The following are the ranges for the alarm status based on Age: • 0 to 30 days • 30 to 60 days • 60 to 90 days • 90 to 120 days The system also displays the source IP Address and descriptions of the alarms.
Information	The status of the application, its synchronization status, and current usage. Current usage lists the number of users and simultaneous administrative logins.
Application State	The current status of the application and its major feature configuration, such as License Status, Deployment Type, Multi-Tenancy, OOBM State, and Hardening Mode.

Options icon ()

Button	Description
Help	Displays the documentation help page.
About	Displays the System Manager Release and build details.
Change Password	Displays the Change Password window.
Log Out	Logs off from the System Manager web console.

Logging on to the System Manager web console

About this task

The System Manager web console is the main interface of Avaya Aura® System Manager. You must log on to the System Manager web console to perform any task. The System Manager home page displays the navigation menu that provides access to shared services to perform various

operations that System Manager supports. The tasks that you can perform from System Manager depend on your assigned role.

Before you begin

Deploy the System Manager OVA.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.

In the security deployments, System Manager displays the Login Warning Banner page.

2. **(Optional)** On the Login Warning Banner page, click **Continue**.
3. In the **User ID** field, type the user name.
4. In the **Password** field, type the password.
5. Click **Log On**.

The system validates the user name and password with the System Manager user account.

- If the user name and password match, the system displays the System Manager home page with the System Manager `<version_number>`.
- If the user name and password do not match, System Manager displays an error message and prompts you to enter the user name and password again.

Once you log in, depending on the system and element configurations, System Manager can display one or more error or notification messages in an Alert Messages pop-up window. For information about these messages, see the “System Manager alert messages at logon” section.

6. Click **OK** to continue.

System Manager message with login details

Important:

From Release 8.1.3.1, System Manager displays the last login information in the **Notifications** widget on the dashboard.

In System Manager Release 8.1.3, after your first successful login, when you log in to the System Manager web console, System Manager displays the Welcome `<SystemManager_UserName>` pop-up window at your every subsequent login.

Note:

When you log in to the System Manager web console for the first time, System Manager does not display the Welcome `<SystemManager_UserName>` pop-up.

Depending on the last successful or unsuccessful login details, System Manager displays the messages in the Welcome `<SystemManager_UserName>` pop-up window.

For example:

```
You have successfully logged into System Manager
```

```
Your last successful login was at <Month> <Date>, <YYYY> <HH:MM> <AM/PM> from <Source_system_IPAddress>
```

```
Your last unsuccessful login was at <Month> <Date>, <YYYY> <HH:MM> <AM/PM> from <Source_system_IPAddress>
```

```
There were <n> unsuccessful login attempts since last successful login
```

If a user logs into the System Manager command-line interface and then logs in to the System Manager web console, then this message also displays the successful and unsuccessful login attempts with the Timestamp and IP address details of the source system.

*** Note:**

After each successful login, on the System Manager web console or CLI, System Manager resets the unsuccessful login count.

- If the login attempt is successful without any unsuccessful login attempt, System Manager displays the following message. For example:

```
You have successfully logged into System Manager
```

```
Your last successful login was at <Month> <Date>, <YYYY> <HH:MM>  
<AM/PM> from <Source_system_IPAddress>
```

```
There were 0 unsuccessful login attempts since last successful login
```

- If the login attempt is successful after one or more unsuccessful login attempts, System Manager displays the following message. For example:

```
You have successfully logged into System Manager
```

```
Your last successful login was at September 16, 2020 11:18 AM from  
13.12.18.24
```

```
Your last unsuccessful login was at September 16, 2020 11:20 AM  
from 13.12.18.24
```

```
There were 1 unsuccessful login attempts since last successful login
```

System Manager alert messages at login

When you log in to the System Manager web console, depending on the system and element configurations, System Manager can display one or more of the following messages.

System Manager license error message

System Manager requires a valid license from Avaya. Use of this software without a valid license is a violation of the Avaya EULA and can result in legal action by Avaya. Please install a System Manager license file on WebLM or immediately discontinue use of this software.

To resolve this error, install the System Manager license file.

System Manager Geographic Redundancy feature entitlement license error message

The System Manager Geo-Redundancy Feature requires a valid license from Avaya with the Geo-Redundancy Feature Entitlement. Use of the System Manager Geo-Redundancy Feature without a valid license from Avaya with the Geo-Redundancy Feature Entitlement is a violation of the Avaya EULA and can result in legal action by Avaya. Please install a System Manager License file on WebLM with the Geo-Redundancy Feature Entitlement or immediately disable use System Manager Geo-Redundancy.

To resolve this error, install the System Manager license file.

Appliance Virtualization Platform license error message

Warning - This instance of Avaya Aura® Appliance Virtualization Platform is currently unlicensed. Note: each instance of Appliance Virtualization Platform is separately licensed and ordered. For example, if you or the Avaya Channel Partner would like to install two instances of the same type of products, then two products of that type must be ordered. Appliance Virtualization Platform is licensed via WebLM with license files obtained from PLDS. Please consult the Appliance Virtualization Platform 7.1.2 or later user documentation for more details onto how to acquire and install a license file. This message will continue to be displayed until the system is correctly licensed. Failure to license the system is in violation of the Avaya Global Software License Agreement for the product. Please immediately place an order using the normal Avaya ordering process to obtain the required license. Avaya Aura® Appliance Virtualization Platform (AVP) License Error Mode: Grace period expires: 01/09/2017 If the grace period expires, AVP will enter License Restricted Mode and AVP Management functionality will be restricted. Check license status on / Home/Services/Solution Deployment Manager (SDM)/Application Management/ Location/Hosts/ for impacted AVP hosts.

If the grace period of the Appliance Virtualization Platform license file is less than 15 days or Appliance Virtualization Platform is in License Error Mode or License Restricted Mode, System Manager displays the AVP License Error message.

For information about Appliance Virtualization Platform license and administration, see *Deploying Avaya Aura® Appliance Virtualization Platform*.

Session Manager emergency Dial Pattern routes message

System Manager displays the following message only on the Release 8.1.3 system:

No Session Manager emergency Dial Pattern routes are administered. To insure proper emergency number handling and routing, please administer Routing Locations, Routing Policies, and Dial Patterns per emergency calling guidelines.

Note:

From Release 8.1.3.1, System Manager displays the Session Manager emergency Dial Pattern routes notification message for Emergency Location Management Solution in the **Notifications** widget on the dashboard.

For information about administering routing locations, routing policies, and dial patterns for emergency calling, see *Administering Avaya Aura® Session Manager*.

Change Password field descriptions

Use this page to change the password for your account.

Name	Description
Current password	The existing password.
New password	The new password that you must set.
Confirm new password	Retype the new password.

Button	Description
Save	Changes the password.
Cancel	Cancels the change password operation and closes the Change Password page.

Logon information for users with administrator privilege

This logon information applies only to users with administrator privilege.

- After installation, when you log on to System Manager for the first time, type the administrator privilege credentials that you created during the deployment or upgrade of System Manager.

The system displays the Forced Change Password page. The Forced Change Password page does not contain the **Cancel** button. You must change the password when you log on to the system using the default password.

Important:

The system displays a message about the invalid logon in the following scenarios:

- Using a disabled account to log on
- Using an invalid password
- Exceeding the maximum number of failed logon attempts limit
- Using an expired password

The password must contain a combination of alphanumeric and special characters. For more information about the password strength policy, see “Password strength policy enforcement”.

Related links

[Password strength policy enforcement](#) on page 60

Certificate based authentication

Certificate-based authentication overview

With System Manager 7.1, you can disable the password-based login and configure the certificate-based authentication for system login. The certificates for this authentication can be issued by:

- System Manager as the default certificate authority
 - Using System Manager user interface
 - Using System Manager CLI
- Third-party certificate authority

Configuring username retrieval from certificate

Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, navigate to **Provision User Certificate Authentication**.
5. Select the **Certificate Purpose**.
6. Select the certificate field names to be used to retrieve the username.
7. Click **Save**.

Enabling certificate-based authentication

Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Configuration > Security Configuration**.
3. On the Security Configuration page, click **SMGR**.
4. In **Cert based authentication** section, enable the required options.

 Caution:

Enabling the **System Manager User Interface** option disables the password-based authentication for the System Manager user interface. The System Manager user interface is accessible using a valid certificate.

5. Click **Commit**.

Creating certificate using System Manager default CA

Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **RA Functions > Add End Entity**.
4. Type the **Username**.
5. Type the **Password** and **Confirm Password**.

The password is mandatory for each end entity. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.

6. Click **Add**.

The system displays the message `End Entity <username> added successfully`.

7. In the navigation pane, click **Public Web**.
8. Click **Create Browser Certificate**.
9. Type the **Username** and **Password**.
10. Click **OK**.
11. Click **Enroll**.
12. **(Optional)** If the certificate is not installed automatically, click **Install Certificate**.

Next steps

If the automatic certificate installation fails, download the certificate and install it in the web browser manually.

Generating certificate from CLI

About this task

Use this procedure to generate a user-specific certificate for System Manager to facilitate the certificate-based authentication.

Before you begin

- To reach the System Manager command line interface, use one of the following methods:
 - Open vSphere Web Client and click on the **Console** tab or the  icon.
 - Use PuTTY.

Procedure

1. Log in to the System Manager command-line interface.
2. Type `getUserAuthCert`, and press `Enter`.
3. Provide the user password and press `Enter`.

4. Type the enrollment password and press `Enter`.
5. Retype the enrollment password and press `Enter`.
6. Type a password for the keystore and press `Enter`.
7. Retype the keystore password and press `Enter`.
8. Type the username and press `Enter`.
9. To generate an identity certificate in the corresponding format, type one of the following and press `Enter`:
 - For `PKCS12` format, type `1`.
 - For `JKS` format, type `2`.
 - For `PEM` format, type `3`.
 - For `PEM-UNENC` format, type `4`.
 - For `PEM-PKCS8` format, type `5`.
 - For `PEM-PKCS8-AES256-CBC` format, type `6`.
10. Press `Enter`.

The system displays the path of the generated identity certificate.
11. Download the certificate and install it in the web browser.

Certificate-based SSH login

Certificate-based CLI access overview

System Manager does not provide a default Command Line Interface (CLI) access to a user. To gain CLI access, an administrator must provide Base OS permissions to the user.

CLI access can be enabled using the following:

- System Manager Web Console
- Putty-CAC

Enabling CLI access using the System Manager web console

Before you begin

Ensure that you add the identity certificate in the browser manually or use an ActivClient tool to add the CAC certificate in the browser.

Procedure

1. Log in to the System Manager web console.
2. On the top-right corner of the System Manager Dashboard, click the **Tool** icon.
3. Click **Manage Command Line Access**.

4. In the System Manager Command Line Access dialog box, click **Enable**.
 - The system creates the user on System Manager OS with the login name provided in the certificate.
 - System Manager Web Console provides CLI access to the user.

Enabling CLI using Putty-CAC

Procedure

1. Download Putty-CAC for certificate-based login from <https://risacher.org/putty-cac/>.
2. Open a putty session.
3. In the **Host name (or IP address)** field, enter the hostname or IP address of System Manager.
4. In the navigation pane, expand the **Connection > SSH**, and click **CAPI**.
Options controlling MS CAPI SSH authentication dialog box opens.
5. Select the **Authentication methods** check box.
6. Click **Browse** to select your identity certificate.

 Note:

Ensure that you add the identity certificate in the browser manually or use an ActivClient tool to add the CAC certificate in the browser.

7. Click **OK** to select the certificate for CAPI Authentication.
8. Click **Open** to start the SSH session.
9. On the CLI, type the username provided in the certificate and press the **Enter** key on the keyboard.
The system displays the pop-up window, Signing data with your private exchange key.
10. On the Signing data with your private exchange key window, click **OK**.
The system provides access to the System Manager CLI.

Tenant Management web console

From the System Manager web console, the user with tenant administrator permissions can perform the following:

- View all tenants in the Tenants panel for which the tenant administrator has permissions. By default, the system selects the first tenant in the list.

Tenants	Level 1	Level 2	Level 3
☒ Citi ☐ BMW	☐ Pune (Citi) ☐ B'lore (Citi) ☐ Cohin (Citi)	☐ Pune HLoan (Pune) ☐ Pune SLoan (Pune)	☐ HLoan Disburse (Pune HLoan) ☐ HLoan Customer (Pune HLoan)

- View all child levels of the selected item in the subsequent panel.
 - When the tenant administrator selects an item, the system:
 - Selects all parent items of the selected item.
 - Displays the child levels of the selected item in the subsequent panel.
 - When the tenant administrator clears all selections in a panel, the system displays the default selection.

*** Note:**

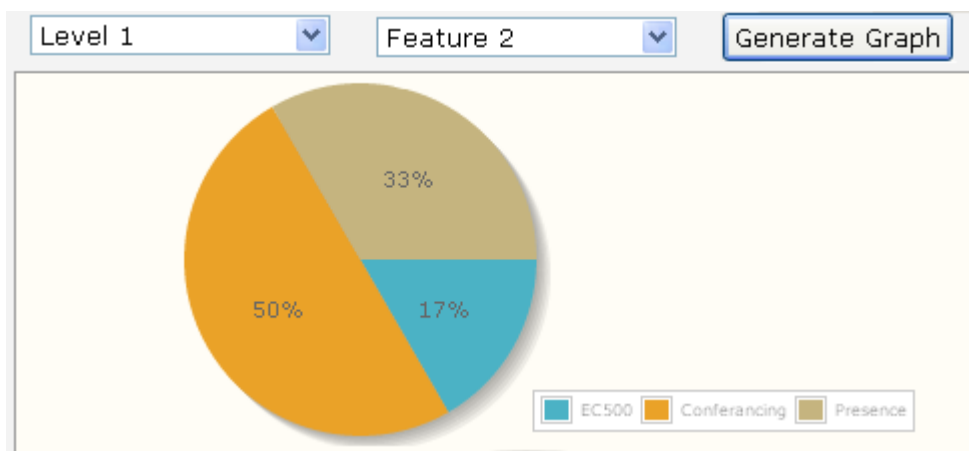
Select at least one tenant. If you do not select a tenant, the system displays a message.

- Gain access to:
 - User Management
 - Communication Manager. Only if the role has permissions to Communication Manager

Navigation	User Provision				
User Management Manage users, shared user resources and provision users Communication Manager Manage Communication Manager 5.2 and higher elements	<table border="1"> <thead> <tr> <th>SIP Users</th> <th>CM Users</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>30</td> </tr> </tbody> </table>	SIP Users	CM Users	1	30
SIP Users	CM Users				
1	30				

- View the **User Provision** section that displays the number of SIP and H.323 users to which the tenant administrator has permissions.
- Select the organizational hierarchy of the tenant and features in the **Graph** section and generate graphs.

The features include EC500, Presence, Conferencing, H.323 users, and SIP users. The system generates Pie charts based on the user selection. If the tenant administrator does not select a level from the Organization level field, the system generates graphs based on items selected in the panels.

**Related links**

[Multi Tenancy](#) on page 1254

Password and security policies for all administrators

Password aging policy enforcement

The password aging policy has the following time-based password thresholds:

- Minimum password age
- Password expiration warning
- Password expiration

The system administrator configures the password threshold in days.

Password threshold	Result of the expiry of the password aging policy threshold
Minimum password age	You cannot change the password until the minimum password age is reached. For example, you cannot change the password within three days after the last change was made.
Password expiration warning	The system sends a password expiration warning when the password is about to expire and before the password expires.
Password expiration period	The system prompts you to change the password after the password threshold expires and before the threshold to disable the account. The password remains locked until the system administrator resets the password.

Password strength policy enforcement

The password strength policy that the system administrator defines enforces the following constraints:

- Passwords must be 6 to 25 characters long. The default character length is 14.
- Passwords must contain a combination of the following characters: a-z, A-Z, 0-9, {, }, |, (,), <, >, ,, /, ., =, [,], ^, _, @, !, \$, %, &, -, +, ", :, ?, `, \, or ;
- Passwords do not require a minimum character type. However, the default is one lowercase, one uppercase, one numeric, and one special character. The sum cannot exceed the minimum total length.
- Password can contain a maximum of 2 consecutive characters. The valid values are from 1 through 5. The default value is 2.
- Password can contain a maximum number of 4 consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4.
- Passwords must not be your user ID, in forward or reverse order.
- Passwords must not be a value based on a dictionary word.

When you enable the password strength policy, if the password does not meet the password strength policy, the system rejects the password.

You can disable the password strength policy.

Password history policy enforcement

The password history policy verifies that a password is new. The blocked passwords can range from 1 to 99. The default value for blocking the number of previous password is 10.

Password lockout policy enforcement

The lockout policy limits the number of unsuccessful attempts that you can make to access System Manager. The system locks System Manager for use after a specified number of login attempts. By default, if you make consecutive attempts within 10 minutes, the system locks you out for 2 minutes after five unsuccessful attempts.

Editing password policies

About this task

A user with the system administrator role can edit the password settings.

Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Policies**.
3. In the **Password Policy** section, click **Edit**.
4. On the Password Policy page, edit the required fields.
5. Click **Save**.

For more information on password policies, contact the system administrator.

6. **(Optional)** To undo your changes and return to the previous page, click **Cancel**.

Related links

[Password policies field descriptions](#) on page 61

Password policies field descriptions

This page is applicable only for users with the username admin.

Aging

Name	Description
Enforce password aging policy	The option to enable or disable the password aging policies. By default, the password aging policy is disabled. To enforce the password aging policies, select the check box. If you clear the check box, the password aging policy is not applicable.
Expiration period	The maximum number of days to maintain the password. The default value is 90. The valid values are from 2 through 365.
Expiration warning	The number of days for password expiry before which the password expiration warning message must be sent to the user. The valid values are from 1 through 15. The default value is 1.
Minimum age for password change	The minimum number of days for password age. The valid values are from 0 through 7. The default value is 3. Ensure that the expiration period is greater than the minimum password age.
Enable expired password change	If this is enabled, you can change the password after it expires. If this is disabled, only the system administrator can change the password. When you log in with the system administrator-provided password, you must change the password.

History

Name	Description
Enforce policy against previously used passwords	The option to enable or disable the password policy against previously used passwords. By default, the password policy against previously used passwords is disabled. To enforce the password policy against previously used passwords, select the check box. If you clear the check box, the password policy against previously used passwords is not applicable.
Previous passwords blocked	The number of latest passwords that the system maintains in history. You cannot reset your password to these values. The valid values are from 1 through 99. From Release 8.1.3, the default value is 10. For earlier release system, the default value is 6.

Strength

Name	Description
Enforce password content standards	The option to enable or disable the password content standards. By default, the password content standards is disabled. To enforce the password content standards, select the check box. If you clear the check box, the password content standards is not applicable.
Minimum total length	The minimum number of characters to use in the password. The password can be of 6 to 25 characters. From Release 8.1.3, the default value is 14. For earlier release system, the default value is 8.
Minimum by character Type: Lower case	The minimum number of lowercase characters to use in the password. The default value is 1.
Minimum by character Type: Upper case	The minimum number of uppercase characters to use in the password. The default value is 1.
Minimum by character Type: Numeric case	The minimum number of numeric characters to use in the password. The default value is 1.
Minimum by character Type: Special case	The minimum number of special characters to use in the password. The default value is 1.

Table continues...

Name	Description
Maximum repeated consecutive characters	The maximum number of repeated consecutive characters. The valid values are from 1 through 5. The default value is 2. For example, if the maximum repeated consecutive characters value is set to 2: - Valid password is: Buildd123\$ - Invalid password is: Builddd123\$
Maximum consecutive characters from same character type	The maximum number of consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4. For example, if the maximum repeated consecutive characters of the same character type is set to 4: - Valid password is: Build123\$ - Invalid password is: Build12345\$

Lockout

Name	Description
Lockout	The option to enable or disable lockout after failed log-in attempts. By default, this is disabled. To enforce the lockout after failed log-in attempts, select the check box. If you clear the check box, the lockout after failed log-in attempts is not applicable.
Consecutive Invalid Login Attempts	The number of failed attempts before the lockout. The valid values are from 1 through 20. The default value is 5.
Interval for Consecutive Invalid Login Attempts	The time interval in minutes between invalid log-in attempts. The valid values are from 0 through 120. The default value is 10.
Lockout Time	The number of minutes that the account must be locked after invalid log-in attempts. The valid values are from 0 through 120. The default value is 2.

For example, with the default values configuration, if you reach up to 5 number of consecutive invalid login attempts within 10 minutes, then the system locks out. After 2 minutes, you can log in.

Within 2 minutes, if you retry to log in, then the timer keeps increasing with the specified limit of 2 minutes.

Button	Description
Save	Saves all the entries on the Edit Password Policies page.
Cancel	Cancels the changes and returns to the previous page.

Managing System Manager password through CLI

setSecurityPolicy command

With Release 8.1.3, you can modify the default password policy settings of System Manager using the **setSecurityPolicy** command. This command is only applicable for changing or setting up the password for the CLI or root user created during deployment.

 Note:

When you create a user through the System Manager web console, the System Manager web console password policy applies.

You can run the **setSecurityPolicy** command in the following modes:

- **Interactive mode:** This is the default mode for operating this command. You can display, change, restore, and refresh the password policy settings.
- **Non-interactive mode:** You can view the status, display the current settings, restore the standard default settings, and refresh the current profile, including any custom settings.

Syntax

```
setSecurityPolicy
```

Displays the interactive mode where you can change the password policy settings.

Syntax

```
setSecurityPolicy [--status] [--display-only] [--restore-standard] [--refresh-custom]
```

--status	Displays the password policy settings status.
--display-only	Displays all the password policy settings.
--restore-standard	Removes all customized values and restores the password policy settings to the default profile settings.
[--refresh-custom]	Refreshes the custom profile settings in case of backup and restore.

Related links

- [Managing the password policies through CLI](#) on page 65
- [Changing the password policies through CLI](#) on page 66
- [Viewing the password policy status](#) on page 68
- [Displaying the password policies](#) on page 69
- [Restoring the default password policy settings](#) on page 69
- [Refreshing the default password policy settings](#) on page 70

Managing the password policies through CLI

Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy**.
3. When the system prompts for the [sudo] password, type the password.

System Manager displays the set of options.

For example:

```
Main Menu:

    Loaded Profile Type: standard
    Custom Profile: yes    (Custom Settings: 1)

1) Display Current Property Settings
2) Change Property Settings
3) Restore Standard Property Settings and Exit
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)

Select Action:
```

Where:

- **Loaded Profile Type:** Specifies the profile selected during deployment. The options are:
 - **standard**
 - **DoD/Hardened**
- **Custom Profile:** The options are:
 - **no:** Specifies that System Manager is using the default values from the loaded profile. This is the default value.
 - **yes:** Specifies that a user has made some changes to customize the security profile.

When the **Custom Profile** setting is **yes**, System Manager displays the **Custom Settings** field with the number of changes made to the default password profile.

For example:

```
Custom Settings: <n>
```

- **Restore Standard Property Settings and Exit:** When you make a change to the password policy settings, System Manager displays this option to remove all the changes and restore the standard property settings to the default values.
4. In **Select Action**, type one of the following:
 - **1:** to display the current property settings.
 - **2:** to change the current property settings.
 - **3:** to restore the standard property settings and exit the command.

- **4:** to refresh the current property settings and exit the command.
- **5:** to exit the command without saving the changes.

Related links

[setSecurityPolicy command](#) on page 64

Changing the password policies through CLI Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy**.
3. When the system prompts for the [sudo] password, type the password.

System Manager displays the set of options.

For example:

```
Main Menu:

    Loaded Profile Type: standard
    Custom Profile: yes    (Custom Settings: 1)

1) Display Current Property Settings
2) Change Property Settings
3) Restore Standard Property Settings and Exit
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)

Select Action:
```

4. In **Select Action**, type 2.

System Manager displays the set of options to change the parameters.

```
Change Property Settings:

    Loaded Profile Type: standard
    Custom Profile: yes    (Custom Settings: 1)

Note: [Current Value: M=modified C=customized D=disabled]

1) Return to Main Menu
2) Change minimum password length [14]
3) Change minimum days between password changes [1]
4) Change maximum days before password expires [-1: D]
5) Change password expiration warning (days) [10]
6) Change minimum required uppercase characters [0: D]
7) Change minimum required lowercase characters [0: D]
8) Change minimum required numeric characters [0: D]
9) Change minimum required special characters [0: D]
10) Change required difference from previous password [4]
11) Change minimum required character classes [3]
12) Change maximum repeated characters [2]
13) Change maximum class repeat [10: C]
14) Change inactive account disable time (days) [0]
15) Change remember previous passwords [10]
16) Change max login attempts before lock out [0: D]
17) Change root lock out allowed [no]
18) Change lock out time (seconds) [900]
```

```
19) Change unlock time (seconds) [600]
20) Change delay (seconds) after failed login attempt [1]
```

Select Action:

5. In **Select Action**, type the number for which you want to change the value.

For example, if you want to change the minimum password length, type 2.

When you type 2, System Manager displays the following prompt.

```
Changing minimum password length:
  Current Value: 14 (Minimum: 6, Maximum: 25)

Enter new value:
```

6. In **Enter new value**, type the required value.

When you type the value, System Manager displays the following prompt with the number of pending changes made.

For example:

```
Change Property Settings:

  Loaded Profile Type: standard
    Custom Profile: yes (Custom Settings: 1)
    Pending Changes: 1

Note: [Current Value: M=modified C=customized D=disabled]

1) Return to Main Menu
2) Change minimum password length [10: M]
3) Change minimum days between password changes [1]
4) Change maximum days before password expires [-1: D]
5) Change password expiration warning (days) [10]
6) Change minimum required uppercase characters [0: D]
7) Change minimum required lowercase characters [0: D]
8) Change minimum required numeric characters [0: D]
9) Change minimum required special characters [0: D]
10) Change required difference from previous password [4]
11) Change minimum required character classes [3]
12) Change maximum repeated characters [2]
13) Change maximum class repeat [10: C]
14) Change inactive account disable time (days) [0]
15) Change remember previous passwords [10]
16) Change max login attempts before lock out [0: D]
17) Change root lock out allowed [no]
18) Change lock out time (seconds) [900]
19) Change unlock time (seconds) [600]
20) Change delay (seconds) after failed login attempt [1]

Select Action:
```

7. To return to the main menu, in **Select Action**, type 1.

System Manager displays the main menu.

For example:

```
Main Menu:

  Loaded Profile Type: standard
    Custom Profile: yes (Custom Settings: 1)
    Pending Changes: 1
```

- ```

1) Display Current Property Settings
2) Change Property Settings
3) Apply Changes and Exit
4) Exit (discarding all pending changes)

```

Select Action:

8. To apply the changes to the password policy settings, in **Select Action**, type 3.

System Manager applies the profile changes, updates the system settings, and displays the number of changes made to the password policy settings.

For example:

```

Loaded Profile Type: standard
 Custom Profile: yes (Custom Settings: 1)
 Pending Changes: 1

Applying Profile Changes:

 Loaded Profile Type: standard
 Custom Profile: yes (Custom Settings: 2)

Updating System Settings:
 Executing pam-settings.sh
 Executing password-policy.sh

```

## Related links

[setSecurityPolicy command](#) on page 64

## Viewing the password policy status

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy --status**, and press Enter.

System Manager displays the password policy status.

Following is the example where the default password policy has not been changed.

```

Loaded Profile Type: standard
Custom Profile: no

```

Following is the example where one setting of the default password policy has been changed.

```

Loaded Profile Type: standard
Custom Profile: yes (Custom Settings: 1)

```

## Related links

[setSecurityPolicy command](#) on page 64

## Displaying the password policies

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **setSecurityPolicy --display-only**, and press Enter.

System Manager displays the configured password policy.

For example:

```
setSecurityPolicy --display-only

Loaded Profile Type: standard
Custom Profile: no
```

| Property                                    | Value | Notes    |
|---------------------------------------------|-------|----------|
| minimum password length:                    | 14    |          |
| minimum days between password changes:      | 1     |          |
| maximum days before password expires:       | -1    | Disabled |
| password expiration warning (days):         | 10    |          |
| minimum required uppercase characters:      | 0     | Disabled |
| minimum required lowercase characters:      | 0     | Disabled |
| minimum required numeric characters:        | 0     | Disabled |
| minimum required special characters:        | 0     | Disabled |
| required difference from previous password: | 4     |          |
| minimum required character classes:         | 3     |          |
| maximum repeated characters:                | 2     |          |
| maximum class repeat:                       | 4     |          |
| inactive account disable time (days):       | 0     |          |
| remember previous passwords:                | 10    |          |
| max login attempts before lock out:         | 0     | Disabled |
| root lock out allowed:                      | no    |          |
| lock out time (seconds):                    | 900   |          |
| unlock time (seconds):                      | 600   |          |
| delay (seconds) after failed login attempt: | 1     |          |

### Related links

[setSecurityPolicy command](#) on page 64

## Restoring the default password policy settings

### About this task

When you make some changes to customize the default password policy and later to restore the default password policy for the current profile, use the following procedure.

- In the Interactive mode, do the following:
  1. Type **setSecurityPolicy**.
  2. When the system prompts for the [sudo] password, type the password.

System Manager displays the set of options.

For example:

```
Main Menu:

Loaded Profile Type: standard
```

```
Custom Profile: yes (Custom Settings: <n>)
```

- ```
1) Display Current Property Settings
2) Change Property Settings
3) Restore Standard Property Settings and Exit
4) Refresh Current Property Settings and Exit
5) Exit (no settings changed)
```

```
Select Action:
```

3. In **Select Action**, type 3.

System Manager updates the system settings and restores the default password policy settings.

```
Loaded Profile Type: standard
Custom Profile: no
```

```
Updating System Settings:
  Executing pam-settings.sh
  Executing password-policy.sh
```

- In the Non-interactive mode, do the following:

1. Type **setSecurityPolicy --restore-standard**, and press Enter.
2. When the system prompts for the [sudo] password, type the password.

System Manager updates the system settings and restores the default password policy settings.

```
Loaded Profile Type: standard
Custom Profile: no
```

```
Updating System Settings:
  Executing pam-settings.sh
  Executing password-policy.sh
```

Related links

[setSecurityPolicy command](#) on page 64

Refreshing the default password policy settings

About this task

When a custom profile is restored during a backup and restore, use the following procedure to apply the changes to the system settings.

- In the Interactive mode, do the following:

1. Type **setSecurityPolicy**.
2. When the system prompts for the [sudo] password, type the password.

System Manager displays the set of options.

For example:

```
Main Menu:
```

```
Loaded Profile Type: standard
Custom Profile: no
```

- ```
1) Display Current Property Settings
```



```

2) Change Property Settings
3) Refresh Current Property Settings and Exit
4) Exit (no settings changed)

```

Select Action:

3. In **Select Action**, type 4.

System Manager refreshes the system settings.

- In the Non-interactive mode, do the following:

1. Type `setSecurityPolicy --refresh-custom`, and press Enter.
2. When the system prompts for the [sudo] password, type the password.

System Manager updates the system settings and refreshes the default password policy settings.

#### Related links

[setSecurityPolicy command](#) on page 64

## Inactive session termination policy

By default, the system suspends a user session after 30 minutes of inactivity. When the session becomes inactive, to access System Manager, you must log on to System Manager again.

## Editing Session Properties

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Policies**.
3. On the Policies page, in the Session Properties section, click **Edit**.
4. On the Session Properties page, edit the required fields.
5. Click **Save**.

#### Related links

[Session Properties field descriptions](#) on page 71

## Session Properties field descriptions

| Name                        | Description                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum Session Time</b> | The maximum time in minutes a session can remain active. The default value is 120. The valid values are 10 through 1440. |

*Table continues...*

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum Idle Time</b>         | <p>The maximum time in minutes a session can remain idle. The default value is 10. The valid values are 10 through 1440.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>You must set the session idle time out to 10 minutes before running a security scan against System Manager using tools like Nessus or IBM AppScan.</li> <li>The maximum idle time must not exceed the maximum session time.</li> </ul> |
| <b>Maximum Sessions Per User</b> | The maximum number of active sessions per user with the same set of credentials. The default is 5. The valid values are 1 through 25.                                                                                                                                                                                                                                                                                                                                                                            |

| Button        | Description                                            |
|---------------|--------------------------------------------------------|
| <b>Save</b>   | Saves the changes on the Session Properties page.      |
| <b>Cancel</b> | Ignores your changes and returns to the previous page. |

## Inactive Account Deactivation Policy field descriptions

| Name                                | Description                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum Inactive Period</b>      | The maximum time in days that a user can remain inactive. The valid values are 7 through 365. The default is 35.                 |
| <b>Account Deactivation Warning</b> | The maximum time in days before which the account deactivation warning is sent. The range is 1 through 60, and the default is 5. |

| Button        | Description                                            |
|---------------|--------------------------------------------------------|
| <b>Save</b>   | Saves the changes made on the current page.            |
| <b>Cancel</b> | Ignores your changes and returns to the previous page. |

## Security settings

System Manager provides a customizable logon banner that appears when a user logs on to the system. Customers who have security policies require the network equipment to display a specific message to users when they log in using the customizable banner.

## Login warning banner

System Manager provides the following:

- Login warning banner: The system administrator can change the text in the login warning banner.

- Additional Postlogin warning banner: In the security deployment, after you log in, System Manager displays a warning banner. You can change only the configurable part of the message.

The Last Login Data window displays the following:

- Last successful login
- Server for the last successful login
- Number of unsuccessful login attempts (if any)

## Editing the login warning banner

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Policies**.
3. On the Policies page, in the Security Settings section, click **Edit**.
4. On the Security Settings page, do the following:
  - a. In the Login Warning Banner area, edit the text as appropriate.
  - b. **(Optional)** For security deployments, in the Additional Post Login Banner Message area, change only the configurable part of the additional text as appropriate.

 **Note:**

You cannot change the actual message. You can change only the configurable part of the post-login banner text.

5. Click **Save**.

## Security Settings field descriptions

| Name                                        | Description                                                                                                                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Login Warning Banner</b>                 | The text displayed during System Manager login. The system administrator can change this text.                                                                                |
| <b>Additional Post Login Banner Message</b> | The text displayed after logging on to System Manager. The text contains two components, the login banner, and the additional text. Only the additional text is configurable. |

| Button        | Description                                            |
|---------------|--------------------------------------------------------|
| <b>Save</b>   | Saves the changes on the Login Warning Banner page.    |
| <b>Cancel</b> | Ignores your changes and returns to the previous page. |

---

## Customized interface

System Manager provides the feature to add a logo to the System Manager web interface. Organizations can customize the logo without removing the Avaya logo.

---

## Adding the corporate logo

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Policies**.
3. On the Policies page, in the **Customized Interface** section, click **Edit**.
4. On the Customized Interface page, in the **Upload File** section, click **Browse** and select an image file to upload.  
  
The system supports PNG, GIF, and JPEG image file formats. The image dimensions must be 100x51 pixels.
5. In the **Change Image ALT Attribute** section, type the alternate text for the system to display.
6. Click **Save**.

System Manager web console displays the corporate logo on the upper-right corner of the page.

### Related links

[Customized Interface field descriptions](#) on page 74

---

## Customized Interface field descriptions

### Upload file

| Button        | Description                                                                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Browse</b> | Displays the File Upload dialog box where you navigate to the image file.<br><br> <b>Note:</b><br>The system supports PNG, GIF, and JPEG file formats. The dimensions of the image must be 100x51 pixels. |

## Change Image ALT Attribute

| Name                | Description                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Image ALT Attribute | <p>The alternate text for the uploaded image.</p> <p> <b>Note:</b></p> <p>The text must be up to 20 characters.</p> |
| Button              | Description                                                                                                                                                                                          |
| Save                | Saves the image on the server and displays the image on the System Manager web console.                                                                                                              |
| Cancel              | Ignores your changes and returns to the previous page.                                                                                                                                               |

---

## Reimporting the SSO cookie domain value

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Policies**.
3. In the Single Sign-on Cookie Domain section, click **Edit**.
4. In **Single Sign-on Cookie Domain**, select the appropriate domain based on the FQDN of the servers you deployed.
5. Click **Save**.
6. Log out and close all browser windows you opened when logging on to the System Manager server.
7. To accept the updated cookies from the new Single Sign-On (SSO) cookie domain name, clear the browser cache.

---

## Administrative users

---

## Viewing administrative user details

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, select the required user ID.

The system displays the User Details page with the administrative user details.

---

## Adding an administrative user

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, click **Add**.  
The system displays the Step 1: Identify the new user page.
4. On the Add New Administrative User page, enter the user ID, full name, and email address.
5. In the **Authentication Type** field, select **Local** or **External**.
6. Do one of the following:
  - In the **Temporary password** and **Re-enter password** fields, type the same password.
  - Click **Generate Password**.

 **Note:**

The auto-generated password applies if **Authentication Type** is set to **Local**.

7. Click **Commit and Continue**.  
The system displays the Step 2: Assign Role(s) page.
8. Select the required roles to be assigned to the user, and click **Commit**.

---

## Editing administrative user details

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, select the required user ID.
4. On the User Details page, make the required changes.
5. Click **Commit**.

---

## Editing administrative user roles

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.

3. On the Administrative Users page, select the required user ID.
4. Click **Select Roles**.
5. On the User Roles page, select the required roles for the administrative user and click **Commit**.

---

## Enabling an administrative user

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, click the required user ID.  
The system displays the User Details page.
4. In **User Status**, click **Enabled**.
5. Click **Commit**.

---

## Disabling an administrative user

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, do one of the following:
  - Select the user, and click **Disable**.
  - Click the required user ID, click **Disabled**, and click **Commit**.

---

## Deleting an administrative user

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, select the users to delete.
4. Click **Delete**.
5. On the Delete Users page, click **Delete** to confirm the user deletion.

---

## Terminating administrative user sessions

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > Administrative Users**.
3. On the Administrative Users page, click **Active Sessions**.
4. On the Active Sessions page, select the sessions to terminate.
5. Click **Terminate**.

---

## Administrative Users field descriptions

| Name           | Description                                                |
|----------------|------------------------------------------------------------|
| User ID        | The unique user identification of the administrative user. |
| Name           | The name of the administrative user.                       |
| Roles          | The list of roles assigned to the administrative user.     |
| Type           | The type of the administrative user.                       |
| Account Status | The status of the administrative user's account.           |

| Button          | Description                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------|
| Add             | Displays the Add New Administrative User page on which you add the administrative users.          |
| Disable         | Use this button to disable the selected administrative users.                                     |
| Delete          | Displays the Delete Users page on which you confirm deletion of selected administrative users.    |
| Active Sessions | Displays the Active Sessions page on which you can terminate active administrative user sessions. |
| Refresh         | Refreshes the element information in the table.                                                   |

---

## Add New Administrative User field descriptions

### Step 1: Identify the new user

| Name    | Description                                            |
|---------|--------------------------------------------------------|
| User ID | Unique user identification of the administrative user. |

*Table continues...*



| Name                       | Description                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Type</b> | The type of authentication. The options are: <ul style="list-style-type: none"> <li>• <b>Local:</b> Avaya Authentication Service performs the user login authentication.</li> <li>• <b>External:</b> The enterprise authenticates the user login.</li> </ul> |
| <b>Full Name</b>           | The full name of the administrative user.                                                                                                                                                                                                                    |
| <b>E-Mail</b>              | The email address of the administrative user.                                                                                                                                                                                                                |
| <b>Temporary Password</b>  | The first-time login password for the administrative user account.                                                                                                                                                                                           |
| <b>Re-enter Password</b>   | The password that you re-enter for confirmation.                                                                                                                                                                                                             |

| Button                     | Description                                                     |
|----------------------------|-----------------------------------------------------------------|
| <b>Generate Password</b>   | Generates a password for the administrative user.               |
| <b>Commit and Continue</b> | Saves the user details and takes you to Step 2: Assign Role(s). |
| <b>Cancel</b>              | Cancels the operation for adding an administrative user.        |

## Step 2: Assign Role(s)

| Button             | Description                               |
|--------------------|-------------------------------------------|
| <b>Role Name</b>   | The name of the role.                     |
| <b>Elements</b>    | The elements that are a part of the role. |
| <b>Description</b> | A description of the role.                |

| Button        | Description                                                                    |
|---------------|--------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the selected user roles for the new administrative user.                 |
| <b>Cancel</b> | Cancels the operation for selecting the roles for the new administrative user. |

# Chapter 3: Directory synchronization

---

## Directory synchronization overview

System Manager integrates with Lightweight Directory Access Protocol (LDAP) directory servers to provide the following functions:

- Synchronization of users from the LDAP directory server to System Manager User Management.
- Bidirectional synchronization of the selected user attributes from System Manager to the LDAP directory server.

LDAP supports the following directory servers for synchronization:

- Microsoft Active Directory 2008
- Microsoft Active Directory 2012
- Microsoft Active Directory 2016
- Microsoft Active Directory 2019
- OpenLDAP 2.4.21
- IBM Domino 7.0
- Novell eDirectory 8.8
- SunOne Directory/Java System Directory 6.3

From the System Manager web console, you can run the directory synchronization engine as an on-demand job. You can also schedule the data synchronization to and from the enterprise directory. During synchronization of information to the enterprise directory server, System Manager modifies the user data that is stored in the LDAP directory server.

From the System Manager web console, you can configure bidirectional attribute mapping through the Directory Synchronization user interface. The bidirectional synchronization does not synchronize the user in the LDAP directory synchronization that is created from the System Manager web console and the System Manager bulk import utility. The bidirectional synchronization only synchronizes the attributes for the user that you synchronized from the LDAP directory server.

You can perform LDAP synchronization of Microsoft Active Directory or other supported directory server administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

### Synchronization by using the user provisioning rule

You can synchronize the communication data, such as extensions, Messaging mail box, and telephone numbers, by using the user provisioning rule. You can map the user provisioning rule to more than one LDAP attribute. However, you cannot map the user provisioning rule to the same LDAP attribute twice.

---

## Results of synchronization from the LDAP directory server to System Manager

You can expect the following results when you run the directory synchronization job or when the system runs the scheduled job.

| Action                                                   | Provided                                                                                                  | Expected result                                              |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Create a new user in the LDAP directory server.          | Add the user in the filter criteria.                                                                      | The system synchronizes the user in System Manager.          |
| Update the user attributes in the LDAP directory server. | The system adds the attributes in the mappings for the data source.                                       | The system updates the user attributes in System Manager.    |
| Change the filter criteria.                              | Remove the user from the filter criteria, and select the <b>Allow Deletion</b> check box.                 | The system permanently deletes the user from System Manager. |
| Delete a user in the LDAP directory server.              | Select the <b>Allow Deletion</b> check box for the data source , and leave the filter criteria unchanged. | The system permanently deletes the user from System Manager. |

---

## Results of synchronization from System Manager to the LDAP directory server

You can expect the following results when you run the directory synchronization job or when the system runs the scheduled job.

| Action                                                                                         | Provided                                                                                                                                           | Expected result                                                      |
|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Update the user attributes that are synchronized from LDAP directory server in System Manager. | The system adds the attributes in the mappings for that datasource, and the mapping synchronizes from System Manager to the LDAP directory server. | The system updates the user attributes in the LDAP directory server. |

---

## Limitations in the synchronization of the LDAP directory server

You can expect the following results when you run the directory synchronization job or when the system runs the scheduled job.

**Table 1: Synchronization from the LDAP directory server to System Manager**

| Action                                                                  | Expected result                                                                                                                                                                                                  |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Synchronize users from multiple LDAP directory servers.                 | The system creates different datasources for each directory server.<br><br>The system supports the authentication of two directory servers, the RADIUS server and the KERBEROS server, at a given point of time. |
| Modify the user attributes that the LDAP directory server synchronizes. | If you add the attributes in mappings for the datasource, the system overwrites the attributes from the synchronization job.                                                                                     |

**Table 2: Synchronization from System Manager to the LDAP directory server**

| Action                                                                                                    | Expected result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a user in System Manager from the User Management interface or by using the bulk import operation. | The system does not synchronize the user in the LDAP directory server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Update the user attributes synchronized from the LDAP directory server in System Manager.                 | If you add the attributes in mappings for the datasource, the system updates the attributes in the LDAP directory server. You can synchronize only optional attributes from System Manager to the LDAP directory server.                                                                                                                                                                                                                                                                                                                               |
| Delete users in System Manager.                                                                           | The system does not delete the user from the LDAP directory server. The Directory Synchronization feature does not support the soft deletion or permanent deletion of the user from the LDAP directory server.<br><br>From System Manager Release 8.0 and later, you can delete the Enterprise/LDAP user from the System Manager web console. However, if the user is still available in the LDAP directory server, the system synchronizes the user in System Manager even after you delete the user from System Manager on next synchronization job. |

---

## Adding the synchronization datasource

### Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.

3. On the User Synchronization page, click the **Synchronization Datasources** tab.
4. Click **New**.
5. On the New User Synchronization Datasource page, complete the fields in the **Directory Parameters** section.
6. Click **Test Connection**.

If the connection fails, the system displays an external directory error message.

If the connection is successful, the system displays the status icon. Click the status icon to view the message. Continue with the next step to map attributes in System Manager to LDAP attributes.

The system displays five mandatory attributes of System Manager that are read-only values.

7. To add more attributes, click **Add Mapping**.

You can use an appropriate LDAP attribute to synchronize in System Manager. If the LDAP attributes that you select are invalid, the synchronization fails.

8. To add the user provisioning rule attribute, perform the following:

- a. Click **Add Mapping**, and select **User Provisioning Rule** from System Manager.

You cannot add the User Provisioning Rule attribute more than one time. After you select **User Provisioning Rule**, the system displays the User Provisioning Rule attribute as read-only.

- b. Select an LDAP attribute that you map to the user provisioning rule.

|   |                   |   |    |                        |        |
|---|-------------------|---|----|------------------------|--------|
|   | registeredAddress | + | -> | User Provisioning Rule | Remove |
| - | postalAddress     | - |    |                        |        |
| - | comment           | - |    |                        |        |

- c. To add more than one LDAP attribute, click plus (+).

You can map more than one LDAP attribute to the user provisioning rule attribute. When you map more than one attribute, the system appends the second and third attributes to the first LDAP attribute. For example, asia\_pune\_maint.

9. Click **Save**.

**\* Note:**

- For bidirectional synchronization of data in the LDAP directory with System Manager, select the two-way arrow icon in the **Attribute Parameters** section.
- The user provisioning rule data synchronization is unidirectional from the LDAP directory server to System Manager.
- In System Manager, you cannot create a user in Active Directory. With bidirectional synchronization, you can only edit the existing user in Active Directory.

During attribute mapping, the right arrow indicates that the system synchronizes from the LDAP server to System Manager. The left arrow indicates that the system synchronizes from System Manager to the LDAP server.

## Related links

[User synchronization datasource field descriptions](#) on page 85

[Results of using the user provisioning rule](#) on page 227

# Editing the synchronization datasource

## Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Datasources** tab and click the record that you must edit.
4. Click **Edit**.
5. On the Edit Synchronization Datasource page, change the required fields.
6. To modify the user provisioning rule attribute:
  - a. To add an LDAP attribute, click the plus (+).

You can map more than one LDAP attribute to the user provisioning rule attribute. When you map more than one attribute, the system appends the second and third attributes to the first LDAP attribute. For example, asia\_pune\_maint.

|                   |   |    |                        |        |
|-------------------|---|----|------------------------|--------|
| registeredAddress | + | -> | User Provisioning Rule | Remove |
| postalAddress     | - |    |                        |        |
| comment           | - |    |                        |        |

You cannot add the User Provisioning Rule attribute more than one time. After you click **User Provisioning Rule**, the system displays the User Provisioning Rule attribute as read-only.

- b. To remove the LDAP attribute, click the minus (-).
7. Click **Save**.

## Related links

[User synchronization datasource field descriptions](#) on page 85

[Results of using the user provisioning rule](#) on page 227

## Deleting a synchronization datasource

### Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Datasources** tab and click a record to delete.
4. Click **Delete**.

 **Note:**

If you synchronize a user by using the datasource that you selected for deletion, the delete operation fails. The system display the message `Data Source <Datasource Name> cannot be deleted as at least one enterprise CsUser references it.`

## User synchronization datasource field descriptions

### Directory Parameters

| Name                           | Example values                                                              | Description                                                                                                                              |
|--------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Datasource Name</b>         | Win2K8ADA                                                                   | The name to identify the directory server. You might require the name later to create a synchronization job.                             |
| <b>Host</b>                    | 111.140.111.126                                                             | The IP address or the host name of the directory server that you synchronize users with.                                                 |
| <b>Principal</b>               | CN=Administrator,<br>CN=Users,DC=pan<br>sv8,DC=platform,D<br>C=avaya,DC=com | The user name of the directory server that has permissions to create or update users.                                                    |
| <b>Password</b>                | <password>                                                                  | The password to connect to the directory server.<br><br>From Release 8.1.3, you can enter up to 256 characters for the directory server. |
| <b>Port</b>                    | 389                                                                         | The port number of the directory<br><br>The default port is 389 for a non-SSL connection and 636 for an SSL connection.                  |
| <b>Base Distinguished Name</b> | CN=Users,DC=pan<br>sv8,DC=platform,D<br>C=avaya,DC=com                      | An element that works with the search scope or the hierarchy from where you synchronize the users.                                       |

*Table continues...*

| Name                             | Example values                     | Description                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LDAP User Schema</b>          | inetOrgPerson                      | The schema that defines object classes by a list of attributes where the values are mandatory or optional. The schema might differ depending on your directory server. The default value is inetOrgPerson.                                                                                                                                                                                             |
| <b>Search Filter</b>             | (cn=Alex*)                         | The field that provides a mechanism to define the criteria for matching entries in an LDAP search operation.<br><br>For more information about Search filter, see <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/aa746475(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/aa746475(v=vs.85).aspx</a> .                                                        |
| <b>Use SSL</b>                   | False when you clear the check box | The option to use SSL to connect to directory server. The default port for an SSL connection is 636.<br><br> <b>Important:</b><br>When you add the certificate, you must select the <b>Import using TLS</b> option.<br><br>For more information about setting up the SSL connection, see Adding trusted certificates. |
| <b>Allow Deletions</b>           | False when you clear the check box | The option to delete a synchronized user that is already removed from the directory server.                                                                                                                                                                                                                                                                                                            |
| <b>Allow Null values in LDAP</b> | False when you clear the check box | The option to allow null values to be inserted by System Manager in LDAP.                                                                                                                                                                                                                                                                                                                              |
| <b>Test Connection</b>           | -                                  | The option to verify your LDAP connection.<br><br>Test the connection before you map attributes.                                                                                                                                                                                                                                                                                                       |

## Attribute Parameters

When you click **Test Connection** and after the test is complete, the system displays the LDAP attributes that you can administer.

When you remove the following attributes from the mapping page, the system does not remove the communication profile handle of the user:

- email
- otherEmail
- Microsoft Exchange Handle
- Microsoft SIP Handle
- IBM Sametime Handle

| LDAP Attribute    | System Manager Attribute | Description                                 |
|-------------------|--------------------------|---------------------------------------------|
| <b>objectGUID</b> | sourceUserKey            | The attribute that uniquely defines a user. |

*Table continues...*



| LDAP Attribute                  | System Manager Attribute                                                                                                                                                                                                           | Description                                                                                                                                                                                                                                   |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>userPrincipalName</b>        | loginName<br><br>* <b>Note:</b><br><br>If you are using Microsoft Active Directory for external authentication with System Manager, the attribute userPrincipalName of the user in the external server must contain a valid value. | The attribute that defines the login name in System Manager.                                                                                                                                                                                  |
| <b>sn</b>                       | surname                                                                                                                                                                                                                            | The attribute that defines the last name of the user.                                                                                                                                                                                         |
| <b>givenName</b>                | givenName                                                                                                                                                                                                                          | The attribute that defines the given name.                                                                                                                                                                                                    |
| <b>displayName</b>              | displayName                                                                                                                                                                                                                        | The attribute that defines the display name.                                                                                                                                                                                                  |
| <b>middleName</b>               | middleName                                                                                                                                                                                                                         | The attribute that defines the middle name.                                                                                                                                                                                                   |
| <b>mail</b>                     | email                                                                                                                                                                                                                              | The attribute that defines the communication profile handle.                                                                                                                                                                                  |
| <b>postalCode</b>               | postalCode                                                                                                                                                                                                                         | The attribute that defines the postal code of the user. The system creates the address of the user, Registered_User_Address.                                                                                                                  |
| <b>streetAddress</b>            | streetAddress                                                                                                                                                                                                                      | The attribute that defines the postal code of the user. The system creates the address for the user with a name.                                                                                                                              |
| <b>preferredLanguage</b>        | preferredLanguage                                                                                                                                                                                                                  | The preferred language of the user.<br><br>Mapping of the LDAP attribute to preferredLanguage must be in the LanguageCode_CountryCode format.<br><br>For the format that the preferredLanguage attribute supports, see “Preferred languages”. |
| <b>mail</b>                     | otherEmail                                                                                                                                                                                                                         | The attribute for the secondary email of the user.                                                                                                                                                                                            |
| <b>roomNumber</b>               | room                                                                                                                                                                                                                               | The room number of the user. The system creates the address of the user, Registered_User_Address.                                                                                                                                             |
| <b>co</b>                       | country                                                                                                                                                                                                                            | The country of the user. The system creates the address of the user, Registered_User_Address.                                                                                                                                                 |
| <b>otherTelephone</b>           | otherBusinessPhone                                                                                                                                                                                                                 | The secondary business telephone number of the user, Registered_User_Address address.                                                                                                                                                         |
| <b>facsimileTelephoneNumber</b> | fax                                                                                                                                                                                                                                | The fax number of the user, Registered_User_Address address.                                                                                                                                                                                  |

*Table continues...*

| LDAP Attribute              | System Manager Attribute  | Description                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>homePhone</b>            | homePhone                 | The residential phone number of the user, Registered_User_Address.                                                                                                                                                                                                                                                                                                  |
| <b>otherHomePhone</b>       | otherHomePhone            | The secondary residential phone number of the user, Registered_User_Address.                                                                                                                                                                                                                                                                                        |
| <b>mobile</b>               | mobilePhone               | The mobile phone number of the user, Registered_User_Address.                                                                                                                                                                                                                                                                                                       |
| <b>otherMobilePhone</b>     | otherMobilePhone          | The secondary mobile phone number of the user, Registered_User_Address.                                                                                                                                                                                                                                                                                             |
| <b>pager</b>                | pager                     | The pager number of the user, Registered_User_Address address.                                                                                                                                                                                                                                                                                                      |
| <b>otherPager</b>           | otherPager                | The secondary pager number of the user, Registered_User_Address.                                                                                                                                                                                                                                                                                                    |
| <b>givenName</b>            | preferredGivenName        | The preferred given name of the user.                                                                                                                                                                                                                                                                                                                               |
| <b>organization</b>         | organization              | The organization to which the user belongs.                                                                                                                                                                                                                                                                                                                         |
| <b>department</b>           | department                | The department to which the user belongs.                                                                                                                                                                                                                                                                                                                           |
| <b>employeeID</b>           | employeeNo                | The employee ID of the user.                                                                                                                                                                                                                                                                                                                                        |
| <b>st</b>                   | stateOrProvince           | The state or the province of the user. The system creates the address of the user, Registered_User_Address.                                                                                                                                                                                                                                                         |
| <b>l</b>                    | localityName              | The locality of the user. The system creates the address for the user, Registered_User_Address.                                                                                                                                                                                                                                                                     |
| <b>displayName</b>          | localizedName             | <p>The localized name of the user in different languages.</p> <p> <b>Note:</b></p> <p>Map the LDAP attribute to localizedName in the format: Locale.Name. For example, if the locale is English and the user name is Alex, the value for <b>displayName</b> must be en.Alex.</p> |
| <b>displayNamePrincipal</b> | endpointDisplayName       | The full text name of the user represented in ASCII. The attribute supports displays that cannot handle localized text, for example, some endpoints.                                                                                                                                                                                                                |
| <b>msExchHomeIdentifier</b> | Microsoft Exchange Handle | The Microsoft Exchange communication address of the user for communication with Microsoft SMTP Server.                                                                                                                                                                                                                                                              |
| <b>o</b>                    | Microsoft SIP Handle      | The Microsoft SIP communication address of the user that supports SIP-based communication.                                                                                                                                                                                                                                                                          |

Table continues...

| LDAP Attribute                  | System Manager Attribute                                                                                                                                                                                                                                                                                                                                                                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>manager</b>                  | IBM Sametime Handle                                                                                                                                                                                                                                                                                                                                                                                                                         | The IBM Sametime communication address of the user that supports IBM Sametime. The format must be of type DN=IBMHandle.                                                                                                                                                                                                                                                                        |
| <b>I</b>                        | User Provisioning Rule<br><br> <b>Note:</b><br>If you map the telephone number (Avaya E164 handle) and UPR in datasource and the LDAP attribute values change in LDAP, during next synchronization, the system updates only the Avaya E164 handle. The system does not update the Communication Manager extension or SIP handle that is configured in UPR. | The user provisioning rule.<br><br>You can map the user provisioning rule to more than one LDAP attribute. The system joins the value of multiple LDAP attributes by an underscore ( _ ) to map the value in System Manager. You cannot map the same LDAP attribute more than once.<br><br>The user provisioning rule data synchronizes from the LDAP directory server to System Manager only. |
| <b>telephoneNumber</b>          | Phone Number                                                                                                                                                                                                                                                                                                                                                                                                                                | The attribute that the system maps to the Avaya E164 handle. The value for the extension is the last N digit value that is set in the <b>Use Phone Number last ..... digits for Extension</b> field on the User Provisioning Rule page.<br><br>The synchronization is bidirectional.                                                                                                           |
| <b>extensionName</b>            | Mailbox Number                                                                                                                                                                                                                                                                                                                                                                                                                              | The Messaging mailbox number.<br><br>The synchronization is bidirectional.                                                                                                                                                                                                                                                                                                                     |
| <b>telexNumber</b>              | CS 1000 Extension                                                                                                                                                                                                                                                                                                                                                                                                                           | The extension on CS 1000, if CS 1000 is supported.<br><br>The data synchronizes from System Manager to the LDAP directory server.                                                                                                                                                                                                                                                              |
| <b>primaryTelexNumber</b>       | Communication Manager Extension                                                                                                                                                                                                                                                                                                                                                                                                             | The extension on Communication Manager.<br><br>The data synchronizes from System Manager to the LDAP directory server.                                                                                                                                                                                                                                                                         |
| <b>msDS-PhoneticLastName</b>    | surnameascii                                                                                                                                                                                                                                                                                                                                                                                                                                | The last name of the user in ASCII.                                                                                                                                                                                                                                                                                                                                                            |
| <b>msDS-PhoneticFirstName</b>   | givennameascii                                                                                                                                                                                                                                                                                                                                                                                                                              | The first name of the user in ASCII.                                                                                                                                                                                                                                                                                                                                                           |
| <b>msDS-PhoneticDisplayName</b> | endPointDisplayName                                                                                                                                                                                                                                                                                                                                                                                                                         | The display name of the user in ASCII as displayed on the endpoint.                                                                                                                                                                                                                                                                                                                            |

*Table continues...*

| LDAP Attribute  | System Manager Attribute | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>memberOf</b> | userRoles                | <p>When synchronized with Enterprise Directory, the roles, rights, and restrictions for administrators are automatically configured for the correct role and inherit the capability of roles.</p> <p>You can map the userRoles attribute to one of the following:</p> <ul style="list-style-type: none"> <li>Groups in LDAP. For example in Active Directory, the attribute memberOf contains the fully qualified group name, such as CN=DnsAdmin,CN=Users,DC=avaya,DC=com. The system searches for DnsAdmin role name.</li> <li>Other LDAP attribute: System searches for the exact name with the value in LDAP attribute that matches with the role in System Manager.</li> </ul> |

| Button        | Description                                                           |
|---------------|-----------------------------------------------------------------------|
| <b>Save</b>   | Adds a new datasource or saves the changes that you made on the page. |
| <b>Cancel</b> | Cancels your action and displays the previous page.                   |

### Related links

[Editing the synchronization datasource](#) on page 84

[Preferred languages](#) on page 90

## Preferred languages

System Manager supports the following locales to set as language preference.

| Language              | Format |
|-----------------------|--------|
| Arabic                | ar     |
| Bulgarian             | bg     |
| Chinese (Simplified)  | zh_CN  |
| Chinese (Traditional) | zh_TW  |
| Czech                 | cs     |
| Danish                | da     |
| Dutch                 | nl     |

*Table continues...*

| Language                 | Format |
|--------------------------|--------|
| English (Canada)         | en_CA  |
| English (United Kingdom) | en_GB  |
| English (United States)  | en_US  |
| Estonian                 | et     |
| Finnish                  | fi     |
| French (Canada)          | fr_CA  |
| French (France)          | fr_FR  |
| German (Germany)         | de_DE  |
| Greek                    | el     |
| Hebrew                   | iw     |
| Hungarian                | hu     |
| Irish                    | ga     |
| Italian (Italy)          | it_IT  |
| Japanese (Japan)         | ja_JP  |
| Korean (Korea)           | ko_KR  |
| Latvian                  | lv     |
| Lithuanian               | lt     |
| Maltese                  | mt     |
| Polish                   | pl     |
| Portugese (Brazil)       | pt_BR  |
| Romanian                 | ro     |
| Russian (Russia)         | ru_RU  |
| Slovak                   | sk     |
| Spanish (Mexico)         | es_MX  |
| Swedish                  | sv     |
| Ukrainian                | uk     |

---

## Creating the user synchronization job

### Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the Active Synchronization Jobs tab.
4. Click **Create New Job**.

5. On the New User Synchronization Job page, select the datasource from which you want to synchronize.
6. Perform one of the following:
  - Click **Run Job** to run the job immediately.
  - Select the **Schedule job for future execution** check box to schedule the job at a later time.

You can delete a job that you scheduled to run in the future.

Every 7 seconds, the system fetches the job status and the number of users synchronized on the Active Synchronization Job tab. Therefore, you might not immediately see the status of the active synchronization job that is running.

#### Related links

[User active synchronization job field descriptions](#) on page 93

---

## Scheduling a user synchronization job

### Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Active Synchronization Jobs** tab.
4. Click **Create New Job**.
5. Perform the following:
  - a. On the New User Synchronization Job page, in the **Datasource Name** field, enter a datasource for which you want to schedule a job.
  - b. Select the **Schedule job for future execution** check box.
  - c. In the **Date** field, enter the date when you want to run the job.
  - d. In the **Time** field, enter the time when you want to run the job.
  - e. In the **Time Zone**, enter the time zone.
  - f. Select the **Repeat Job Execution** check box to repeat the job
  - g. Select the recurring interval in minutes, hours, days, weeks, or months.
6. Click **Schedule job for future execution**.

## Deleting a user synchronization job

### Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Job History** tab and select the job that you want to delete.
4. Click **Delete Job**.

Without any confirmation, the system deletes the job.

 **Note:**

You can delete a job that is scheduled to run in the future.

## User active synchronization job field descriptions

| Name                                     | Description                                       |
|------------------------------------------|---------------------------------------------------|
| <b>Datasource Name</b>                   | The name of the datasource                        |
| <b>Schedule job for future execution</b> | The option to schedule a user synchronization job |
| <b>Date</b>                              | The date on which you want to schedule the job    |
| <b>Time</b>                              | The time when you want to schedule the job        |
| <b>Time Zone</b>                         | The time zone closest to your location            |

| Button                                   | Description                                                                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Run Job</b>                           | Runs the user synchronization job that you specified.                                                                                                |
| <b>Schedule job for future execution</b> | Schedules a user synchronization job.<br>The system displays the button only when you select the <b>Schedule job for future execution</b> check box. |
| <b>Cancel</b>                            | Cancels the synchronization and displays the previous page.                                                                                          |

## Synchronization job history

The **Synchronization Job History** tab displays the history of jobs created for user synchronization and the result of each job execution. You can delete any entry from the list of user synchronization job by using the **Delete Job** link.

**Related links**

[Synchronization job history field descriptions](#) on page 94

---

## Synchronization job history field descriptions

| Name              | Description                                                                                                                                                                                           |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>       | The datasource name for which the user synchronization job was executed.                                                                                                                              |
| <b>Start Time</b> | The start time of a user synchronization job.                                                                                                                                                         |
| <b>End Time</b>   | The time when a user synchronization job was completed.                                                                                                                                               |
| <b>Status</b>     | The status of the user synchronization job.                                                                                                                                                           |
| <b>Job Result</b> | The result of running a job.<br><br>To view the results of the user synchronization, click the <b>View Job Summary</b> link. The system displays the results on the Synchronization Job Summary page. |
| <b>Action</b>     | The <b>Delete Job</b> link that you use to delete the results of the user synchronization job.                                                                                                        |

| Icon                                                                                | Description                                                              |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
|  | Refreshes the information on the <b>Synchronization Job History</b> tab. |

---

## Viewing Job Summary

### Procedure

1. On the System Manager web console, click **Users > Directory Synchronization**.
2. In the navigation pane, click **Sync Users**.
3. On the User Synchronization page, click the **Synchronization Job History** tab.
4. In the **Job Result** column, click the **View Job Summary** link.

**Related links**

[Viewing Job Summary field descriptions](#) on page 95



## Viewing Job Summary field descriptions

| Name                           | Description                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Datasource Name</b>         | The datasource name for which the user synchronization job was run.                                                                                                                                                                                               |
| <b>End Time</b>                | The time when the user synchronization job was completed.                                                                                                                                                                                                         |
| <b>Job Results</b>             | The results of running the user synchronization job.                                                                                                                                                                                                              |
| <b>Added</b>                   | The number of users added to the system as a result of running the job.<br>For a nonzero count, the system displays an expand sign (+) or collapse sign (-). You can click the sign to show or hide the details of user entries.                                  |
| <b>Modified</b>                | The number of users modified as a result of running the job.<br>For a nonzero count, the system displays an expand or collapse sign. You can click the sign to show or hide the details of modified user entries.                                                 |
| <b>Deleted</b>                 | The number of users deleted as a result of running the job.<br>For a nonzero count, the system displays an expand or collapse sign. You can click the sign to show or hide the details of deleted user entries.                                                   |
| <b>Unchanged</b>               | The number of users that remained unchanged after running the job.                                                                                                                                                                                                |
| <b>Failed</b>                  | The number of user records that the system failed to synchronize because of errors. For a nonzero count, the system displays an expand or collapse sign. You can click the sign to show or hide the details of user entries for which the synchronization failed. |
| <b>Total records processed</b> | The total number of user records that the system processed while the job is in progress.                                                                                                                                                                          |

| Button      | Description                 |
|-------------|-----------------------------|
| <b>Back</b> | Displays the previous page. |

# Chapter 4: Geographic Redundancy

---

## Geographic Redundancy overview

Avaya Aura® provides System Manager Geographic Redundancy, a resiliency feature that handles scenarios where the primary System Manager server fails or the data network partially loses connectivity. In such scenarios, the system manages and administers products such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager across the customer enterprise using the secondary System Manager server.

For customers who need highly fault-tolerant deployments, System Manager supports System Manager Geographic Redundancy deployments that can provide the Active-Standby mode of resiliency.

From Release 8.0.1, System Manager also supports Geographic Redundancy in a mixed deployment environment. The deployment environment can be any of the following:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Aura® Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 6.5.
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure and Kernel-based Virtual Machine (KVM).
- Avaya Aura® on Infrastructure as a Service: Amazon Web Services, Microsoft Azure, Google Cloud Platform, and IBM Bluemix.
- Software-only environment: Deployment on the Red Hat Enterprise Linux operating system.

From Release 7.0.1, System Manager supports deployment on different server types and different deployment modes in Geographic Redundancy. System Manager supports mixed:

- Server constructs of Small, Medium, and Large Common Server Release 1, 2, and 3 constructs that are defined for use with System Manager Release 7.x. For example, the primary System Manager server is on the Medium CSR2 and the secondary System Manager server is on the Small CSR2.
- System Managers in a standalone and shared modes between the primary and secondary System Manager on Common servers. This includes allowing any combination of Avaya Aura® applications running with the primary and secondary System Manager instances.
- Servers from any combination of CSR1, CSR2, and CSR3 servers.
- Servers from both customer-provided virtualized environment and Appliance Virtualization Platform.

For example, the primary System Manager server can be on Appliance Virtualization Platform and the secondary System Manager server can be on a customer-provided virtualized environment.

The following are some key differences between Geographic Redundancy and High Availability (HA) solutions:

| Geographic Redundancy                  | HA                                                                                           |
|----------------------------------------|----------------------------------------------------------------------------------------------|
| Addresses sudden, site-wide disasters. | Addresses server outages due to network card, hard disk, electrical, or application failure. |
| Distributed across WAN.                | Deployed within a LAN.                                                                       |
| Manual                                 | Automated                                                                                    |

You must install System Manager on both the standalone servers with separate IP addresses and configure Geographic Redundancy. If a managed product that supports the Geographic Redundancy feature loses connectivity to the primary System Manager server, the secondary System Manager server provides the complete System Manager functionality. However, you must manually activate the secondary System Manager server.

 **Note:**

Only the system administrator can perform Geographic Redundancy-related operations.

You must reconfigure the elements that do not support Geographic Redundancy so that the elements can interact with the secondary System Manager server to receive configuration information. For more information about configuring elements that do not support Geographic Redundancy, see *Geographic Redundancy-unaware elements overview*.

During the installation of GR-unaware elements such as Presence Server, you must specify whether you want to enable the Geographic Redundancy feature on the element.

### Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

#### Related links

[Geographic Redundancy-unaware elements overview](#) on page 131

---

## Licensing in Geographic Redundancy

In Geographic Redundancy, the system replicates the license file on the secondary System Manager server that you installed on the primary System Manager server. When you activate the

secondary System Manager server, the same license file works on the secondary System Manager server.

In Geographic Redundancy, you must generate the license file by using the host ID of primary System Manager.

---

## Geographic Redundancy terminology

### **Primary System Manager server**

The first or the master System Manager server in a Geographic Redundancy setup that serves all system management requests.

### **Secondary System Manager server**

The System Manager server that functions as a backup to the primary System Manager server in a Geographic Redundancy setup. The secondary System Manager server provides the full System Manager functionality when the system fails to connect to the primary System Manager server.

### **Active System Manager server**

The mode of operation of the System Manager server where the server provides the full System Manager functionality.

### **Standby System Manager server**

The mode of operation of the System Manager server where the server serves only authentication and authorization requests. In the standby mode of operation, the system supports limited Geographic Redundancy configuration, the inventory service.

### **Standalone System Manager server**

The single System Manager server deployed in an enterprise that provides full System Manager functionality. The standalone server operates independently and does not contain a backup server.

### **Element**

An element is an instance of an Avaya Aura® network entity that the System Manager manages. For example, a Session Manager server or a Communication Manager server.

In the context of System Manager Geographic Redundancy, the elements can be classified as follows:

- **Geographic Redundancy-unaware element:** An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.2.x and earlier. If you have a Geographic Redundancy-unaware element that is configured and managed by the primary System Manager server, and if the primary System Manager goes down or a Split brain scenario occurs, then you cannot use the secondary System Manager to manage the element either automatically or with a simple click of a button. If you need to manage a Geographic Redundancy-unaware element, then you need to make the changes manually. The manual changes differ from one Geographic Redundancy-unaware element to another.

- **Geographic Redundancy-aware element:** An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3 and later. These elements can leverage the services of the primary or the secondary System Manager servers, either automatically or with the simple click of a button. The Geographic Redundancy-aware elements are classified in the following types:

- Elements capable of automatically switching between the primary and secondary System Manager servers depending on the state of the System Manager servers - If the primary System Manager server goes down or a Split brain scenario occurs and you activated the secondary System Manager server, then the element can detect it and depending on the current state of the System Manager server, the element automatically switches to the appropriate System Manager server, so that the element can be managed by it.

For example, if you have a System Manager 8.1.x Geographic Redundancy deployment, (Sunny Day) with a few Session Manager 8.1.x servers configured and you activated the secondary System Manager due to a network split, then each Session Manager server detects this. If the primary System Manager is not reachable, then the Session Manager server automatically switches to the active secondary System Manager server. If the primary System Manager server is reachable, then the element does not switch to the secondary System Manager, even though it is active. This does not mean that you cannot manage them. To manage the element through the secondary System Manager server, on secondary System Manager go to the Manage Elements page, select the element, and then click the **More Options > Force Manage** option.

- Elements that require manual switch - If the primary System Manager server goes down or a Split brain scenario occurs, and you need to manage the element from the secondary System Manager server, then on secondary System Manager go to the Manage Elements page, select the element, and then click the **More Options > Force Manage** option. This step is required to manage such elements from the secondary System Manager server.

### Geographic Redundancy-aware element

An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3.

### Geographic Redundancy-unaware element

An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager release earlier than 6.3.

### Geographic Redundancy operational modes

- **The normal operation mode.** Also called the Sunny Day scenario. A System Manager Geographic Redundancy scenario where the primary System Manager server runs in the active mode while the secondary System Manager server runs in the standby mode providing limited set of services. In the normal operation mode, the primary System Manager server manages all elements and provides the complete System Manager functionality.
- **Primary nonoperational mode.** Also called the Rainy Day scenario. The primary System Manager server fails or loses connectivity to all elements that the system manages. The administrator activates the secondary System Manager server to make the secondary System Manager server manage all elements in the system.
- **Split network.** A System Manager Geographic Redundancy scenario when the primary and secondary System Manager servers run in the active mode but cannot communicate with each other due to a network connectivity outage or when some elements cannot

communicate with one System Manager and both primary and secondary System Manager servers can communicate with each other.

### Failover

Failover is the process of activating the secondary System Manager server when the primary System Manager server becomes nonoperational due to server outage or loses connectivity to the elements that the server manages.

### Failback

Failback is the process of making the primary System Manager server operational by restoring the primary System Manager server by using the primary or secondary System Manager data.

---

## Geographic Redundancy replication

The Geographic Redundancy feature provides the following replication mechanisms to ensure consistency of data between the primary and the secondary System Manager servers:

- Database replication
- File replication
- LDAP (Directory) replication

The primary System Manager server continuously replicates the data with the secondary System Manager server. If the system does not replicate the data for a specific period of time that is configured in **Services > Configurations > Settings > SMGR > HealthMonitor**, the primary and the secondary System Manager servers raise alarms.

---

## Prerequisites for the Geographic Redundancy setup

In a Geographic Redundancy setup, the two standalone System Manager servers that you designate as primary and secondary servers must meet the following requirements:

- Contain the same version of the software that includes software packs.
- Contain the same profile for primary and secondary System Manager Geographic Redundancy virtual machines. For example, if the primary System Manager contains Profile 2, the secondary System Manager must also contain Profile 2.
- Contain the same version of the System Manager software that includes service pack and software patches.
- Contain the same parent domain names for two System Manager systems. For example, smgr.abc.com and smgr.xyz.com are invalid domain names because the parent domain names abc and xyz are different.
- Communicate with each other over the network by using the IP address and FQDN.

- In the Geographic Redundancy setup, the primary and secondary System Manager must use the same VFQDN.
- Have a synchronized network time.
- Use DNS to ensure that the name resolution is automatic. Otherwise, you must resolve the IP address and the host name in the `/etc/hosts` file on the primary and secondary System Manager servers.
- Have open required ports to support the Geographic Redundancy feature. For port usage information, see *Avaya Port Matrix: Avaya Aura® System Manager* on the Avaya Support website at <http://support.avaya.com/>.
- Have T1 as the minimum data pipe between the primary and the secondary System Manager server. T1 provides 1.544 Mbps.
- Have network latency that is less than 500 ms.
- In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.

## Hardware resource and parameter for the Geographic Redundancy setup

| # | Hardware Resource or Parameter    | Similar on Primary and Secondary? (Mandatory or Recommended) | Does System Manager take care? | Notes                                                                                                                                                                        |
|---|-----------------------------------|--------------------------------------------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 64 bit architecture               | Mandatory                                                    | No                             | Require 64 bit system for both servers.<br><br>Require x86_64 architecture to support System Manager provided operating system and then for the Geographic Redundancy setup. |
| 2 | Byte Order (Big or Little endian) | Mandatory                                                    | Yes                            | This depends on CPU architecture.                                                                                                                                            |
| 3 | 64 bit OS                         | Mandatory                                                    | Yes                            | -                                                                                                                                                                            |
| 4 | PostgreSQL major version          | Mandatory                                                    | Yes                            | -                                                                                                                                                                            |
| 5 | PostgreSQL minor version          | Recommended                                                  | Yes                            | -                                                                                                                                                                            |

Table continues...

| #  | Hardware Resource or Parameter | Similar on Primary and Secondary? (Mandatory or Recommended) | Does System Manager take care? | Notes                                                                                                                                                                                                                                          |
|----|--------------------------------|--------------------------------------------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6  | Number of CPUs                 | Recommended                                                  | No                             | Mandatory CPU reservation: <ul style="list-style-type: none"> <li>• Profile 2: 6</li> <li>• Profile 3: 8</li> <li>• Profile 4: 18</li> </ul> Validated along with profile validation during Geographic Redundancy configuration.               |
| 7  | Memory                         | Recommended                                                  | No                             | Mandatory memory reservation: <ul style="list-style-type: none"> <li>• Profile 2: 12 GB</li> <li>• Profile 3: 18 GB</li> <li>• Profile 4: 36 GB</li> </ul> Validated along with profile validation during Geographic Redundancy configuration. |
| 8  | Storage                        | Recommended                                                  | No                             | Mandatory Total storage of 120 GB is required for profile 2<br>Validated along with profile validation during Geographic Redundancy configuration.                                                                                             |
| 9  | System Manager profile         | Mandatory                                                    | Yes                            | System Manager validates during Geographic Redundancy configuration.                                                                                                                                                                           |
| 10 | System Manager version         | Mandatory                                                    | Yes                            | System Manager validates during Geographic Redundancy configuration.                                                                                                                                                                           |
| 11 | Synchronized Time              | Mandatory                                                    | Yes                            | System clock and hardware clock must be set if required keeping synchronized Time on primary and secondary.<br><br>System Manager validates during Geographic Redundancy configuration.                                                        |



# Key tasks for Geographic Redundancy

## Prerequisites

Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

## Key tasks

Only the system administrator can perform Geographic Redundancy-related operations.

- Configure Geographic Redundancy.

Configure Geographic Redundancy to handle the situation when the primary System Manager server fails or when the managed element loses connectivity to the primary System Manager server.

### Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

- Enable the Geographic Redundancy replication between the two servers.

Enable the replication in the following scenarios:

- After you configure the two standalone System Manager servers for Geographic Redundancy, you must enable the Geographic Redundancy replication between the two servers to ensure that the secondary System Manager server contains the latest copy of the data from the primary System Manager server.
- During the system maintenance or upgrades, Geographic Redundancy replication must be disabled. After maintenance activity is complete, you must enable Geographic Redundancy replication if it was manually or automatically disabled due to the maintenance activity.

### Note:

If the heartbeat between the two System Manager servers in which the Geographic Redundancy replication is enabled stops due to network connectivity failure or the server failure, the system automatically disables the Geographic Redundancy replication within a preconfigured time. The default is 5 minutes. If the primary and secondary System Manager servers are running and if the network connectivity between the two servers fails, the system triggers auto-disable on both servers. If one of the two servers becomes nonoperational, the system triggers auto-disable on the server that is operational.

- After the primary System Manager server recovers from failure.

### Important:

During the bulk activities such as import, export, and full synchronization of Communication Manager, the system might disable the Geographic Redundancy replication for reasons, such as the size of the data involved in the bulk activity and the bandwidth between the primary and the secondary System Manager server. After you

complete the bulk activity, enable the Geographic Redundancy replication if the replication is disabled.

- Disable the Geographic Redundancy replication between the two servers.

Disable the Geographic Redundancy replication before you start the maintenance activities such as upgrades, installation of software patches or hot fixes. If the primary and the secondary System Manager servers disconnect from each other for more than the threshold period, the system automatically disables the Geographic Redundancy replication. The default threshold period is 5 minutes.

- Activate the secondary System Manager server.

Activate the secondary System Manager server in the following scenarios:

- The primary System Manager becomes nonoperational.
- The enterprise network splits.

- Deactivate the secondary System Manager server.

Deactivate the secondary System Manager server in the following situations:

- The primary System Manager server becomes available.
- The element network restores from the split.

- Restore the primary System Manager server.

After you activate the secondary System Manager server, to return to the active-standby mode, you must restore the primary System Manager server. You can choose to restore from the primary System Manager or the secondary System Manager server.

 **Note:**

The system does not merge the data from the primary and secondary server.

- Reconfigure Geographic Redundancy.

You can reconfigure Geographic Redundancy when the secondary System Manager is in the standby mode or active mode. The reconfiguration process copies the data from the primary System Manager server to the secondary System Manager server.

- Convert the primary System Manager server to the standalone server.

Perform this procedure to convert the primary System Manager server in the Geographic Redundancy-enabled system to a standalone server or if you have to configure a new secondary server.

For detailed instructions to complete each task, see the appropriate section in this document.

# Prerequisites before configuring Geographic Redundancy

## Geographic Redundancy prerequisites overview

Before enabling and configuring Geographic Redundancy, do the following:

1. Configure CRL download on the secondary System Manager server.

 **Note:**

By default, CRL is valid only for 7 days. Therefore, you must configure Geographic Redundancy before the expiry date of CRL.

2. Add the trusted certificate of primary server to the secondary System Manager server.
3. If certificate is replaced on Primary Server by third-party signed certificate then same certificate type must be replaced on Secondary Server by same third-party CA.  
  
For example: If *Management Container TLS Service* is replaced by third-party CA signed certificate on Primary Server then same type certificate must be replaced on Secondary Server by same third-party CA.
4. Install third-party certificate on both servers prior to Geographic Redundancy configuration and post Geographic Redundancy configuration.  
  
For more information, see “Managing certificates”.
5. Ensure that third-party CA certificate is added into trust store of both System Manager.
6. Replaced certificate must have full chain (id certificate ->inter CA (if present) certificate -> root CA certificate) and also must contain correct FQDN/VFQDN in required places.
7. Configure CRL download is mandatory for Geographic Redundancy.
8. If CRL URL for third-party is not accessible from System Manager, then set **Certificate Revocation Validation** from **BEST\_EFFORT** to **NONE** on the **Security > Configuration > Security Configuration > Revocation Configuration** page.

JBoss service automatically restarts after 10 minutes.

### Related links

[Configuring CRL download on the secondary System Manager server](#) on page 107

[Adding the trusted certificate of primary server to the secondary System Manager server](#) on page 108

[Configuring CRL download on the secondary System Manager server](#) on page 107

[Adding the trusted certificate of primary server to the secondary System Manager server](#) on page 108

---

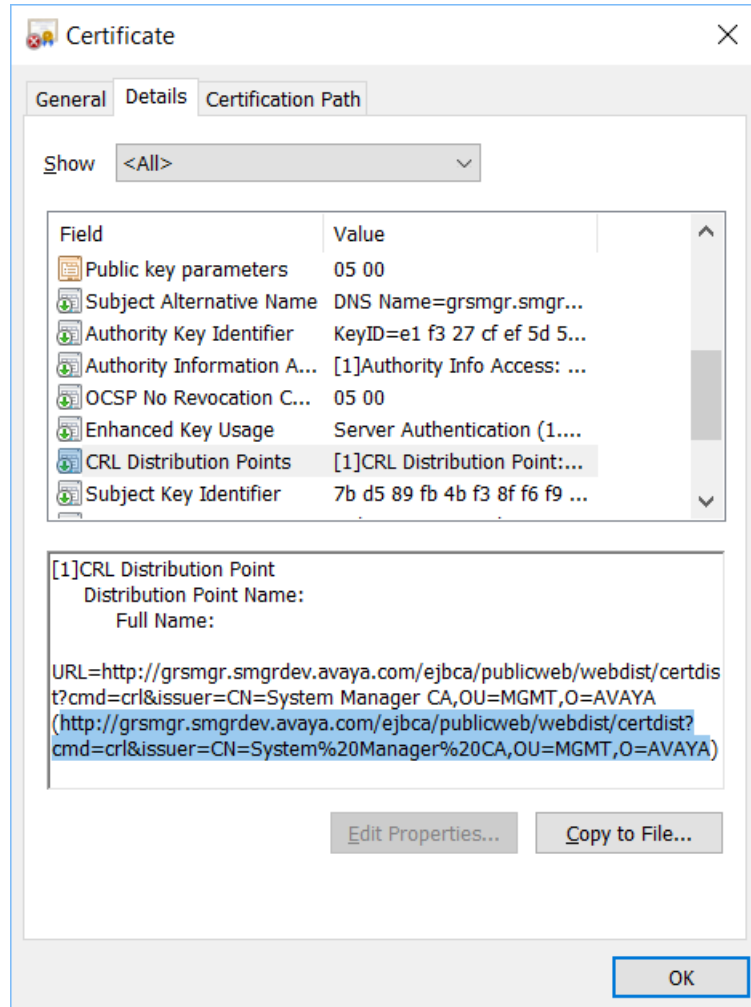
## Copying the CRL URL

### Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name>/SMGR`, the System Manager URL.
2. On the address bar, click the Lock icon.
3. Click **View certificates**.
4. On the Certificate dialog box, do the following:
  - a. Click on the **Details** tab.
  - b. Scroll down and click the **CRL Distribution Points** field.

The system displays the CRL URL in the text box.

For example: `http://<vFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA`



- c. Press **Ctrl+C** and copy the URL in Notepad for configuring CRL download in the Geographic Redundancy set up.
- d. Click **OK**.

## Configuring CRL download on the secondary System Manager server

### Procedure

1. Access the login page of the primary System Manager server.
2. Copy the CRL of the browser certificate.

For information about copying the CRL URL, see “Copying the CRL URL.”

3. Replace the vFQDN in the CRL with the IP address of the primary System Manager server.

For example, the CRL in the certificate is:

```
http://<vFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

The new CRL for the certificate will be:

```
http://<ip-address>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

Where, <vFQDN> and <ip-address> are the respective vFQDN and IP address.

 **Note:**

If you installed a third-party certificate on System Manager servers, this step is not required. If third-party certificate, then configure CRL URL of the third-party certificate for CRL download.

4. Log on to the secondary System Manager web console.
5. On the System Manager web console, click **Services > Security**.
6. In the navigation pane, click **Configuration > CRL Download**.
7. On the CRL Download Configuration page, click **Add**.

The system displays the Schedule CRL Download page.

8. In **Job Name**, type the job name.
9. In **Job Frequency**, set the frequency and recurrence to schedule the job within a few minutes after the CRL addition.

For more information, see Schedule CRL Download field descriptions.

10. Copy the new CRL URL from Notepad and paste the URL in the **Configure CRL Distribution Point** field.

For information about copying the CRL URL, see “Copying the CRL URL.”

CRL URL example:

```
http://<ip-address>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

11. Click **Add**, and then click **Commit**.

Ensure that the job is completed successfully.

## Next steps

Add the trusted certificate of primary server to the secondary System Manager server.

---

# Adding the trusted certificate of primary server to the secondary System Manager server

## Procedure

1. Log in to the primary System Manager web console.

2. On the System Manager web console, click **Services > Security**.
3. In the navigation pane, click **Certificates > Authority**.
4. Click **CA Functions > CA Structure & CRLs**.
5. Click **Download PEM file**.
6. Log in to the secondary System Manager web console.
7. On the System Manager web console, click **Services > Inventory**.
8. In the navigation pane, click **Manage Elements**.
9. On the Manage Elements page, select the System Manager certificate and click **More Actions > Manage Trusted Certificates**.
10. On the Manage Trusted Certificates page, click **Add**.
11. Click **Choose File** and select the previously downloaded PEM file.
12. Click **Retrieve Certificate**, and then click **Commit**.

---

## Configuring Geographic Redundancy

### Before you begin

- For the new installation of System Manager, ensure that you change the default password for the system administrator user.
- Ensure that you change CLI passwords on primary and secondary System Manager servers.  
60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.
- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

### About this task

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

#### Important:

- During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.
- After the Geographic Redundancy configuration is complete, the credentials used for logging in to the secondary System Manager becomes identical to the login credentials of the primary System Manager.

## Procedure

1. Log on to the System Manager web console of the standalone server that you require to designate as the secondary server and perform the following:

- a. On the System Manager web console, click **Services > Geographic Redundancy**.
- b. Click **Configure**.
- c. In the dialog box, provide the details of the primary System Manager server in the following fields:

- **Primary Server Username**

Enter the system administrator user name that you use to log on to the primary System Manager server.

- **Primary Server Password**

Enter the system administrator password that you use to log on to the primary System Manager server.

- **Primary Server IP**

- **Primary Server FQDN**

- d. Click **OK**.

The configuration process takes about 30 minutes. However, the duration might vary depending on the size of the data on the primary System Manager server.

 **Note:**

Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

The server that you configured becomes the secondary server and the other standalone server becomes the primary System Manager server.

2. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:

- Log on to the web console of the primary System Manager server and perform the following:
  - a. On the System Manager web console, click **Services > Geographic Redundancy**.
  - b. Refresh the GR Health page.

If **Enable** is available, the configuration is complete.

 **Note:**

Log off and log on to the primary System Manager server to view the updated status of Geographic Redundancy health.



- Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following:

a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

```
SMGR :: operationStatus=success

SMGR :: Quantum has been successfully
configured as a secondary.
```

### Next steps

On the web console of the primary System Manager server, enable the Geographic Redundancy replication.

### Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Geographic Redundancy field descriptions](#) on page 120

---

## Enabling the Geographic Redundancy replication

Enable the Geographic Redundancy replication between the two servers to ensure that the data gets continuously replicated between the primary and secondary System Manager servers.

### Before you begin

- Log on to the System Manager web console of the primary server.
- Ensure that CLI passwords on primary and secondary System Manager servers do not expire.

60 days after the System Manager CLI password expires, Geographic Redundancy becomes nonoperational. You must set a new password on primary and secondary System Manager servers for Geographic Redundancy to become operational again.

### About this task

#### Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

### Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy**.
2. Click **Enable Replication**.

The system displays the progress information in the **Enable GR Status** section.

 **Note:**

Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

If the enabling process is successful, the system displays the Geographic Redundancy replication status as `Enabled`. If the process fails, the system displays an error message with the replication status as `Failed` on the primary the System Manager web console. The primary server remains in the failed state while the secondary server rolls back to the previous state. Verify if the system has raised an alarm for a temporary network connectivity failure. Retry when the network connectivity is restored. If the problem persists, contact Avaya service personnel.

**Related links**

[Geographic Redundancy field descriptions](#) on page 120  
[Disabling the Geographic Redundancy replication](#) on page 112  
[Activating the secondary System Manager server](#) on page 113  
[Changing the TLS version of System Manager](#) on page 1168  
[Deactivating the secondary System Manager server](#) on page 114  
[Restoring the primary System Manager server](#) on page 115  
[Converting the primary System Manager server to the standalone server](#) on page 119  
[Re-establishing trust for Solution Deployment Manager elements](#) on page 1356

---

## Disabling the Geographic Redundancy replication

### Before you begin

Log on to the System Manager web console of the primary server.

### Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy**.
2. Click **Disable Replication**.
3. In the dialog box, click **Yes**.

The system displays the progress information in the **Disable GR Status** section.

If the disabling process is successful, the system displays the Geographic Redundancy replication status as `Disabled`. The system stops replicating the data from the primary and secondary System Manager server. If the disabling process fails, the system displays an error message on the web console of the primary System Manager.

**Related links**

[Geographic Redundancy field descriptions](#) on page 120  
[Activating the secondary System Manager server](#) on page 113

[Changing the TLS version of System Manager](#) on page 1168

[Deactivating the secondary System Manager server](#) on page 114

[Restoring the primary System Manager server](#) on page 115

[Enabling the Geographic Redundancy replication](#) on page 111

---

## Activating the secondary System Manager server

### About this task

- When you activate the secondary System Manager server, the system stops replicating the data from the primary System Manager server to the secondary System Manager server. During activation, you cannot gain access to the web console of the secondary System Manager server for some time.
- In the same browser instance, do not open the primary and secondary System Manager server in different tabs. The system might display an unknown error after the activation, deactivation, or recovery is complete. You can ignore this error message.

### Before you begin

Log on to the System Manager web console of the secondary server.

### Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy > GR Health**.
2. Click **Activate Secondary Server**.

The system displays the Geographic Redundancy (GR) Health Current status dialog box.

3. In the Select the reason for activation, choose one of the following options:
  - **Primary Down:** When the primary System Manager server becomes nonoperational, the server hardware is faulty and unusable, or the application server fails to recover.
  - **Network Split:** When the enterprise network splits and servers fail to communicate with each other.
  - **Maintenance:** When the maintenance activities such as backup, restore, upgrade, and shutdown are in progress.
  - **Other:** Any other reason where the primary System Manager server becomes unusable and needs the secondary System Manager server to become operational.

4. Click **Yes**.

The system displays the initialization of the activation process.

5. Click **Yes**.

The activation process takes about 15–20 minutes to complete.

If the activation process fails, the system displays an error message on the secondary System Manager web console and rolls back to the previous state. If the activation process

is successful, the secondary System Manager server changes to the active mode and provides complete System Manager functionality.

Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

#### Related links

- [Geographic Redundancy field descriptions](#) on page 120
- [Disabling the Geographic Redundancy replication](#) on page 112
- [Changing the TLS version of System Manager](#) on page 1168
- [Deactivating the secondary System Manager server](#) on page 114
- [Restoring the primary System Manager server](#) on page 115
- [Enabling the Geographic Redundancy replication](#) on page 111

---

## Deactivating the secondary System Manager server

### Before you begin

Log on to the System Manager web console of the secondary server.

### Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy > GR Health**.
2. Click **Deactivate Secondary Server**.

The system displays the Deactivate Secondary Server dialog box and the progress while performing the deactivation process.

3. Click **OK**.

If the deactivation process is complete, the secondary System Manager server goes to the standby mode. If the deactivation process fails, the system displays an error message on the secondary System Manager web console and the server remains in the active mode.

### Next steps

Restore primary System Manager. For information, see “Restoring the primary System Manager server”.

#### Related links

- [Geographic Redundancy field descriptions](#) on page 120
- [Disabling the Geographic Redundancy replication](#) on page 112
- [Activating the secondary System Manager server](#) on page 113
- [Changing the TLS version of System Manager](#) on page 1168
- [Restoring the primary System Manager server](#) on page 115
- [Enabling the Geographic Redundancy replication](#) on page 111

---

# Restoring the primary System Manager server

## Before you begin

Log on to the System Manager web console of the primary server.

## About this task

You can restore the data when the secondary System Manager server is active or in the standby mode. However, for minimum system nonfunctional time during data restoration or an emergency or both, you can restore the data when the secondary System Manager server is active.

### Important:

After you restore the system with the secondary System Manager data, if you want to revert to the primary System Manager data, you can restore to the primary System Manager data using the procedure in Step 4. However, you must restore to the primary System Manager data, before you enable the Geographic Redundancy replication. After you enable the Geographic Redundancy replication, you cannot restore to the primary System Manager server data.

## Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy**.
2. Click **Restore Data**.
3. On the Restore GR dialog box, select a server whose data you want to retain:

- **Primary Server**

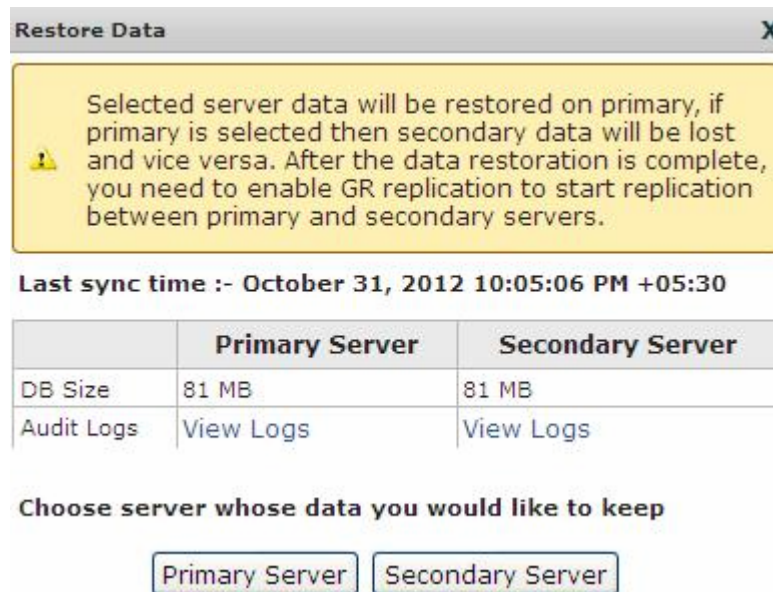
The system keeps the primary System Manager server data. The data on the secondary System Manager server is lost.

Select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between activation and deactivation and the administrator wants to retain those changes even after restoring the data using **Restore Data**.

- **Secondary Server**

The system restores the data from the secondary server on the primary System Manager server. the System Manager web console is unavailable for some time. The time that the system takes to restore depends on the network speed and the size of the data that the system must restore.

After the system recovery, select the secondary System Manager server if the secondary System Manager server data changes significantly during the interval between the system recovery and the deactivation and if you want to retain the changes from the secondary System Manager server after restoring the data by using **Restore Data**.



The system displays the Restore Status dialog box.

The system displays the restore operation status and the status of the primary and the secondary System Manager server.

**! Important:**

After you restore the data, all changes that you make on the secondary System Manager server that is active will not be available on the primary System Manager server.

4. If you later decide to revert to the database of the primary System Manager server, perform the following steps after the restore is complete:
  - a. Using the command line interface, log in to System Manager of the primary server with administrator privilege CLI user credentials.
  - b. Change to the `$MGMT_HOME/geo/bin` directory.
  - c. Type `sh backupandrestore.sh recovery secondaryIP secondaryFQDN`.

When the script completes, System Manager restarts and contains the data from the primary System Manager server that was available before you restored with the secondary System Manager data.

**\* Note:**

- To restore with the secondary System Manager server data again, activate and deactivate the secondary System Manager server.
- Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

## Next steps

Verify the data and deactivate the secondary System Manager server if the server is active during the restoration process.

Enable the Geographic Redundancy replication to synchronize the primary and secondary System Manager servers.

## Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Deactivating the secondary System Manager server](#) on page 114

[Geographic Redundancy field descriptions](#) on page 120

[Disabling the Geographic Redundancy replication](#) on page 112

[Activating the secondary System Manager server](#) on page 113

[Changing the TLS version of System Manager](#) on page 1168

[Deactivating the secondary System Manager server](#) on page 114

[Enabling the Geographic Redundancy replication](#) on page 111

---

# Reconfiguring Geographic Redundancy

## Before you begin

- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.
- Log on to System Manager web console of the secondary server.

## About this task

For resiliency, from the pair of standalone System Manager servers, you can configure Geographic Redundancy.

### Important:

During the configuration of Geographic Redundancy, the primary System Manager replicates the data between the primary and the secondary System Manager servers. Therefore, ensure that the system maintenance activities such as backup, restore, and shutdown are not in progress.

## Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy**.
2. Click **Reconfigure**.
3. In the dialog box, provide the details of the primary System Manager server in the following fields:

- **Primary Server Username**

Enter the admin user name that you use to log on to the primary System Manager Web console.

- **Primary Server Password**

Enter the admin password that you use to log on to the primary System Manager Web console.

- **Primary Server IP**

- **Primary Server FQDN**

4. Click **OK**.

 **Note:**

Because the server becomes unavailable, you cannot gain access to the web console. Wait until the process is complete before you continue with the next step.

The server that you configured becomes the secondary server and the other standalone server becomes the primary System Manager server.

5. To view the status of the Geographic Redundancy configuration during the restart of the two application servers, perform one of the following:

- Log on to the web console of the primary System Manager server and perform the following:
  - a. On the System Manager web console, click **Services > Geographic Redundancy**.
  - b. Refresh the GR Health page.

If **Enable** is available, the configuration is complete.

 **Note:**

Log off and log on to the primary System Manager server to view the updated status of Geographic Redundancy health.

- Log in to the secondary System Manager server as system administrator by using the command line interface and perform the following:

- a. Type `tail -f /home/ucmdeploy/quantum/autoReconfig.log`.

The system displays the progress during the restart of the two application servers. When the second application server restart completes, the system displays the following messages:

```
SMGR :: operationStatus=success

SMGR :: Quantum has been successfully
configured as a secondary.
```

## Next steps

On the primary the System Manager Web console, enable the Geographic Redundancy replication.



---

## Converting the primary System Manager server to the standalone server

### Before you begin

- Log on to the System Manager web console of the primary server.
- Disable the Geographic Redundancy replication if you have not already disabled.

### Note:

You can also reconfigure secondary System Manager to the standalone server by performing the same steps.

### Procedure

1. On the System Manager web console, click **Services > Geographic Redundancy**.
2. Select the primary System Manager server, and click **Convert To Standalone**.

The system displays a dialog box.

3. Click **OK**.

If the conversion is successful, the system displays `Converted to Standalone successfully` and converts the primary System Manager server to a standalone server.

The system displays the status of the server as `Unconfigured` on the Manage Elements page. The administrator can configure the server when required.

### Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Geographic Redundancy field descriptions](#) on page 120

---

## About the Health Monitoring service

Using the Health Monitoring service, you can monitor the status of the following:

- Database replication
- File replication
- LDAP replication
- System health check
- Application server

The system checks the condition of services on both the primary and secondary System Manager servers.

You can configure the following parameters from **Services > Configurations > Settings > SMGR > HealthMonitor** of the System Manager web console:

- Health monitoring interval
- The number of days the health monitoring data must be retained
- The number of successive retries before an alarm is raised

You can configure the timeout interval for health monitoring in the `MonitorConfig.properties` file from System Manager CLI. The properties file is available in the `$MGMT_HOME/SystemMonitor/res/` location. The default timeout interval is 15 seconds.

The health monitoring includes the overall status of the replication, and the detailed health metric such as the time and size of the data that the secondary System Manager server lags in replication behind the primary System Manager server.

You can view the heartbeat status and the health monitoring details in the graphical format for different services from **View Heartbeat Status** from **Services > Geographic Redundancy > GR Health** on System Manager web console.

### Related links

[Configuring the timeout interval for health monitoring](#) on page 120

[View Profile:HealthMonitor field descriptions](#) on page 880

[Edit Profile:HealthMonitor field descriptions](#) on page 881

[GR Health field descriptions](#) on page 122

---

## Configuring the timeout interval for health monitoring

### Procedure

1. Log in to System Manager CLI.
2. From the `$MGMT_HOME/SystemMonitor/res` location, open the `MonitorConfig.properties` file.
3. In the properties file, change the value for the `ServiceTimeOutInterval` property.  
The default is 15 seconds.
4. To restart the service, type `service systemMonitor restart`.  
The changes take effect.

---

## Geographic Redundancy field descriptions

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

## Primary Server Details

The system displays the IP address and the FQDN of the primary System Manager server.

| Name                         | Description                                                                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Convert to Standalone</b> | Converts to a standalone server.<br><br>The system displays the <b>Convert to Standalone</b> button only when the replication is disabled. |
| <b>Configure</b>             | Configures Geographic Redundancy.<br><br>The system displays the <b>Configure</b> button only on the standalone System Manager server.     |
| <b>Reconfigure</b>           | Configures Geographic Redundancy.<br><br>The system displays the <b>Reconfigure</b> button only on the secondary System Manager server.    |

## Secondary Server Configured

You can use the **Enable Replication**, **Disable Replication**, and **Restore Data** buttons only from the primary System Manager server.

| Button                     | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Replication</b>  | Continuously replicates the data between the primary and the secondary System Manager server.<br><br>The system displays the <b>Enable Replication</b> button after the following events: <ul style="list-style-type: none"> <li>• State of Geographic Redundancy is Disable.</li> <li>• Geographic Redundancy configuration.</li> <li>• Restoration of the primary Geographic Redundancy server is complete.</li> </ul> |
| <b>Disable Replication</b> | Stops replicating the data between the primary and the secondary System Manager server.<br><br>The system displays the <b>Disable Replication</b> button when the state of Geographic Redundancy is Enable.                                                                                                                                                                                                              |
| <b>Restore Data</b>        | Recovers the server after the failback.<br><br>The system displays the <b>Restore Data</b> button when the secondary System Manager server is deactivated.                                                                                                                                                                                                                                                               |

| Name                      | Description                                                                         |
|---------------------------|-------------------------------------------------------------------------------------|
| <b>IP</b>                 | Displays the IP address of the secondary System Manager server.                     |
| <b>FQDN</b>               | Displays FQDN of the secondary System Manager server.                               |
| <b>Replication Status</b> | Displays the status of replication. The values are Disabled and Enabled.            |
| <b>Last Action</b>        | Displays the last action that you performed on the secondary System Manager server. |

*Table continues...*

| Name                      | Description                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------|
| <b>Last Action Status</b> | Displays the status of the last action that you performed on the secondary System Manager server. |

## GR Health field descriptions

The information available on the GR Health page is read-only.

The Geographic Redundancy and the GR Health pages remain blank on a standalone server or until you configure a secondary System Manager.

### GR Health

| Name                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GR Health Status</b>            | <p>Displays the health status of the monitored services. The page displays:</p> <ul style="list-style-type: none"> <li>• , if the monitored service stops.</li> <li>• , if the monitored service is running.</li> <li>• , if the monitored service fails to run.</li> </ul>                                |
| <b>Activate Secondary Server</b>   | <p>Click to make the secondary server provide full System Manager functionality when the primary System Manager server fails, or the data network splits.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• The system displays <b>Activate Secondary Server</b> only on the secondary System Manager server.</li> <li>• The system displays the <b>Activate Secondary Server</b> or the <b>Deactivate Secondary Server</b> button on the page.</li> </ul> |
| <b>Deactivate Secondary Server</b> | <p>Click to make the primary System Manager resume operation. You use this option when the primary System Manager server restores operation or recovers from a network failure.</p> <p> <b>Note:</b></p> <p>The system displays <b>Deactivate Secondary Server</b> only on the secondary System Manager server.</p>                                                                                                                                                        |
| <b>Service Name</b>                | Displays the name of the service for which the system provides the status of the health.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

*Table continues...*

| Name               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Detail</b> | <p>Click <b>View Graph</b>.</p> <ul style="list-style-type: none"> <li>For database and directory replication, the system displays the graph for default interval. If no graph is present for the default interval, using the calendar, you can set the period for which you require to check the health status, and click <b>Generate</b> to view health details in a graph.</li> </ul> <p>For database replication, the system displays graphs for time lag and the size lag. For directory replication, the system displays graph for time lag only.</p> <ul style="list-style-type: none"> <li>For file replication, the system displays the last replication time and the size of the lag.</li> </ul> |

## HeartBeat status

Click **View Heartbeat Status** to view the details. The system displays the GR Heartbeat page.

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service Name</b>                   | <p>The name of the monitored service. The services are:</p> <ul style="list-style-type: none"> <li><b>System Health:</b> The heartbeat status indicates if the primary or the secondary System Manager server can communicate with the peer System Manager server over the network.</li> <li><b>Database Replication:</b> The heartbeat status indicates if the data stored in the System Manager database is getting replicated between the primary and the secondary System Manager server.</li> <li><b>Application System Health:</b> The heartbeat status indicates if the application server of primary or secondary System Manager can query the application server of the peer System Manager.</li> <li><b>File Replication:</b> The heartbeat status indicates if the configuration files are getting replicated between the primary and the secondary System Manager server.</li> <li><b>Directory Replication:</b> The heartbeat status indicates if the data stored in the internal LDAP server is getting replicated in the respective System Manager server.</li> </ul> |
| <b>Last Successful Heartbeat Time</b> | The last time the heartbeat was successful for the monitored service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Last Missed Heartbeat Time</b>     | The last time when the monitored service missed the heartbeat.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>View Details</b>                   | <p>The <b>View Graph</b> link to view the health status of the monitored service over a period of time. To configure the time period, click <b>Edit Dates</b>. The graph displays the status in 0 and 1.</p> <ul style="list-style-type: none"> <li>0 indicates that the monitored service is either stopped or failed at that point of time</li> <li>1 indicates that the monitored service is running at that point of time.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

---

## Prerequisites for configuring disaster recovery

---

### Disaster recovery prerequisites

To configure the disaster recovery for the primary System Manager server:

1. Set up a new primary System Manager server.
2. Configure CRL download on the primary System Manager server.

 **Note:**

By default, CRL is valid only for 7 days. Therefore, you must configure disaster recovery before the expiry date of CRL.

3. Add the trusted certificate of the secondary System Manager server to the new primary System Manager server.
4. If certificate is replaced on Primary Server by third-party signed certificate then same certificate type must be replaced on Secondary Server by same third-party CA.  
  
For example: If *Management Container TLS Service* is replaced by third-party CA signed certificate on Primary Server then same type certificate must be replaced on Secondary Server by same third-party CA.
5. Install third-party certificate on both servers prior to Geographic Redundancy configuration and post Geographic Redundancy configuration.  
  
For more information, see “Managing certificates”.
6. Ensure that third-party CA certificate is added into trust store of both System Manager.
7. Replaced certificate must have full chain (id certificate ->inter CA (if present) certificate -> root CA certificate) and also must contain correct FQDN/VFQDN in required places.
8. Configure CRL download is mandatory for Geographic Redundancy.
9. If CRL URL for third-party is not accessible from System Manager, then set **Certificate Revocation Validation** from **BEST\_EFFORT** to **NONE** on the **Security > Configuration > Security Configuration > Revocation Configuration** page.

JBoss service automatically restarts after 10 minutes.

---

## Configuring CRL download on the primary System Manager server

### Procedure

1. Access the login page of the secondary System Manager server.
2. Copy the CRL of the browser certificate.

For information about copying the CRL URL, see “Copying the CRL URL.”

3. Replace the vFQDN in the CRL with the IP address of the secondary System Manager server.

For example, the CRL in the certificate is:

```
http://<vFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

The new CRL for the certificate will be:

```
http://<ip-address>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=System%20Manager%20CA,OU=MGMT,O=AVAYA
```

Replace the <vFQDN> and <ip-address> tags with the respective vFQDN and IP address.

 **Note:**

If you installed a third-party certificate on System Manager servers, this step is not required. If third-party certificate, then configure CRL URL of the third-party certificate for CRL download.

4. Log on to the primary System Manager web console.
5. On the System Manager web console, click **Services > Security**.
6. In the navigation pane, click **Configuration > CRL Download**.
7. On the CRL Download Configuration page, click **Add**.

The system displays the Schedule CRL Download page.

8. In **Job Name**, type the job name.
9. In **Job Frequency**, set the frequency, and recurrence to schedule the job within a few minutes after the CRL addition.

For more information, see Schedule CRL Download field descriptions.

10. In **Configure CRL Distribution Point**, type the new CRL.
11. Click **Add**, and then click **Commit**.

Ensure that the job is completed successfully.

### Next steps

Add the trusted certificate of the secondary System Manager server to the new primary System Manager server.

## Adding the trusted certificate of secondary server to the primary System Manager server

### Procedure

1. Log in to the secondary System Manager web console.
2. On the System Manager web console, click **Services > Security**.
3. In the navigation pane, click **Certificates > Authority**.

4. Click **CA Functions > CA Structure & CRLs**.
5. Click **Download PEM file**.
6. Log in to the primary System Manager web console.
7. On the System Manager web console, click **Services > Inventory**.
8. In the navigation pane, click **Manage Elements**.
9. On the Manage Elements page, select the System Manager certificate and click **More Actions > Manage Trusted Certificates**.
10. On the Manage Trusted Certificates page, click **Add**.
11. Click **Choose File** and select the previously downloaded PEM file from the secondary server.
12. Click **Retrieve Certificate**, and then click **Commit**.

---

## Replacing System Manager servers

---

### Replacement of System Manager servers

From the pair of System Manager servers that are configured with Geographic Redundancy, you might have to replace the primary System Manager server with a new primary System Manager server or move existing primary System Manager server to a different location. The following sections list the scenarios when you must replace the primary System Manager server and the key tasks involved in the replacement procedure.

---

### Moving the existing primary System Manager server to a different location

#### Procedure

1. Disable the Geographic Redundancy replication.
2. Shut down the System Manager server, and relocate the server to a new location.
3. **(Optional)** Activate the secondary System Manager server.

You activate the secondary server to ensure zero down time. If you do not activate the secondary server, do not perform Step 7 and Step 8.
4. Start the primary System Manager server.
5. If the primary System Manager server uses a different IP or FQDN or both, change the IP address, FQDN, or both on the primary System Manager server.



For instructions to change the IP address or FQDN, see [Changing the IP address and FQDN in System Manager](#).

6. Connect the primary System Manager server to the network.
7. Deactivate the secondary System Manager server if you already activated in Step 3.
8. Restore the data.
9. Enable the Geographic Redundancy replication.

#### Related links

- [Enabling the Geographic Redundancy replication](#) on page 111
- [Restoring the primary System Manager server](#) on page 115
- [Deactivating the secondary System Manager server](#) on page 114
- [Disabling the Geographic Redundancy replication](#) on page 112
- [Activating the secondary System Manager server](#) on page 113

---

## Restoring the primary System Manager server using the old primary server backup data

### About this task

When the primary System Manager server or the site fails, you can restore the primary System Manager server using the backup data from the old primary server.

### Procedure

1. **(Optional)** Activate the secondary System Manager server.  
Activate the secondary server to ensure zero down time. If you do not activate the secondary server, do not perform Step 6 and Step 7.
2. On the new server, install the System Manager template that you later designate as primary server by using the cold standby procedure.  
For information about how to change over to the cold standby server, see *Upgrading Avaya Aura® System Manager*.
3. If you must to use a different IP address or FQDN or both on the new primary System Manager server, change the IP address, FQDN, or both on the primary System Manager server. For more information, see [Changing the IP address and FQDN in System Manager](#).
4. Connect the primary System Manager server to the network if not already connected to the network.
5. Deactivate the secondary System Manager server.
6. Restore the data.
7. Enable the Geographic Redundancy replication if not already enabled.

## Related links

- [Enabling the Geographic Redundancy replication](#) on page 111
- [Deactivating the secondary System Manager server](#) on page 114
- [Disabling the Geographic Redundancy replication](#) on page 112
- [Activating the secondary System Manager server](#) on page 113
- [Recovering the primary System Manager server from disaster](#) on page 129

---

## Restoring the primary System Manager server using the data on the secondary System Manager server

When the primary System Manager server or the site fails, you can restore the primary System Manager server using the data on the secondary System Manager server.

### Procedure

1. Activate the secondary System Manager server if you have not already activated.
2. Create a backup of the secondary System Manager server.
3. On the new server, install the System Manager template and perform the following steps:
  - a. Log on to the System Manager web console of the standalone server that you installed, and change the admin password.  
Ensure that the server meets the requirements for the Geographic Redundancy setup.
  - b. Recover System Manager from disaster.
4. Deactivate the secondary System Manager server.
5. Restore the data.
6. Enable the Geographic Redundancy replication.

## Related links

- [Enabling the Geographic Redundancy replication](#) on page 111
- [Deactivating the secondary System Manager server](#) on page 114
- [Disabling the Geographic Redundancy replication](#) on page 112
- [Activating the secondary System Manager server](#) on page 113
- [Recovering the primary System Manager server from disaster](#) on page 129

---

## Replacing the secondary System Manager server on the site

### About this task

From the pair of System Manager servers that are configured with Geographic Redundancy, you might have to replace the secondary System Manager server with a new secondary System

Manager server or move existing secondary System Manager server to a different location. The reasons might be the following:

- Secondary System Manager failure
- Site failure
- Movement of the secondary to a different location.

## Procedure

1. Create a backup of the primary System Manager server.
2. On System Manager web console, click **Services > Replication** and verify that the system synchronized all elements to the primary System Manager server the data replication is working.
3. On the new server, install the System Manager template. For instructions, see *Implementing Avaya Aura® System Manager*.
4. Convert the primary System Manager server to standalone server.
5. On System Manager web console, click **Services > Replication** and verify that the system synchronized all elements to the primary System Manager server the data replication is working.
6. Log on to System Manager web console of the standalone System Manager server that you installed and change the password.
7. Configure Geographic Redundancy.
8. Enable the Geographic Redundancy replication if you have not already enabled.

## Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Configuring Geographic Redundancy](#) on page 109

[Converting the primary System Manager server to the standalone server](#) on page 119

---

## Recovering the primary System Manager server from disaster

Perform the system recovery process when the primary System Manager server becomes unavailable and when you do not have a backup to restore on the new System Manager server.

### About this task

#### Important:

During the system recovery of Geographic Redundancy, the active secondary System Manager server copies the data from the secondary System Manager server to the primary System Manager server. Therefore, ensure that the system maintenance activities, such as, backup, restore, and shutdown are not in progress.

### Before you begin

- For fresh installation of System Manager, change the default password for the system administrator user.

- Ensure that the two System Manager servers meet the requirements that are defined in Prerequisites for servers in the Geographic Redundancy setup.

## Procedure

1. Activate the secondary System Manager server.
2. Create a backup of the secondary System Manager server.
3. View and verify the virtual FQDN that is configured on the secondary System Manager server by using one of the following:
  - From the virtual FQDN configured in the System Manager certificate, do one of the following:
    - On Firefox, click the  icon on the address bar of the browser. Click **More Information > View Certificate > Details**. In the **Certificate Details** area, click **Certificate > Extensions > Certificate Subject Alt Name**. The system displays two values for **DNS Name**. The first entry is the virtual FQDN.
    - On Internet Explorer, click **Certificate Error** next to the address bar and click **View Certificates > Details > Subject Alternative Name**. The first entry for **DNS Name** is the virtual FQDN.
  - From the command line interface, log in to the secondary System Manager server, and check the virtualFQDN property value in the `$MGMT_HOME/infra/conf/smgr-properties.properties` file.
4. On the new server, install the System Manager template that you later designate as primary server with the same virtual FQDN that you obtained in Step 3.
5. Log on to the web console of the new System Manager server to change the default password.
6. For Release 7.1 and later, perform the steps provided in the “Disaster recovery prerequisites” section.
7. Log in to the command line interface of the newly created primary System Manager with administrator privilege CLI user credentials, and perform the following:
  - a. Perform one of the following:
    - For Releases 6.3.1 and 6.3.0, type `sh $MGMT_HOME/geo/bin/rundisasterrecovery.sh <peer fqdn> <peer ip> <peerNodesmgrUserId> <peerNodesmgrPassword>`.
    - For Release 6.3.2 and later, type `sh $MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN <secondary fqdn> -IP <secondary IP> -ID <secondary System Manager web console system admin user name> -PASS <secondary System Manager web console system admin password>`.
    - For Release 7.1 and later, type `sudo -u admin $MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN <SECONDARY_HOST_NAME> -IP <Secondary_Host_IPAddress> -ID admin -PASS <UIPassword>`

Release 6.3.x example: `$MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN psvdbf24.dr.sdr.com -IP 144.235.244.244 -ID systemadmin -PASS System$567.`

Release 7.1.x example: `sudo -u admin $MGMT_HOME/geo/bin/rundisasterrecovery.sh -FQDN sit2.smgrdev.avaya.com -IP 2a07:2a42:adc0:1d::87 -ID admin -PASS System$675`

The recovery process starts and takes about 40 minutes. The command runs in the background and the system creates nohup logs in the directory from where you run the `rundisasterrecovery.sh` command, which you can tail.

b. Type one of the following:

- `tail -f $AVAYA_LOG/mgmt/geo/disasterRecoveryScript.log`
- `tail -f nohup.out`

8. To quit the `tail` command, press `Control+C`.

When the recovery process is complete, the system displays the message `Disaster Recovery has completed JBoss will be restarted`, may take up to 15 minutes. The system configures System Manager servers as a Geographic Redundancy pair with the secondary data on the primary System Manager server.

9. Deactivate the secondary System Manager server.
10. Restore the data from the primary System Manager server.
11. Enable the Geographic Redundancy replication.

The system starts working in the normal operational mode.

#### Related links

- [Enabling the Geographic Redundancy replication](#) on page 111
- [Restoring the primary System Manager server](#) on page 115
- [Deactivating the secondary System Manager server](#) on page 114
- [Activating the secondary System Manager server](#) on page 113

---

## Configuring the GR-unaware elements to work with System Manager

---

### Geographic Redundancy-unaware elements overview

Geographic Redundancy-unaware (GR-unaware) elements are elements that cannot support the System Manager Geographic Redundancy feature. GR-unaware elements might be legacy

elements, that is, prior to Release 6.3, which are already present in the field or elements that have not yet leveraged the Geographic Redundancy feature.

You must manually activate the secondary System Manager server to manage the elements when:

- The primary System Manager server fails.
- The network fails to isolate one of the System Manager systems or one or more adopter elements or both.

This scenario is called the primary nonoperational scenario or rainy day scenario.

This document provides the procedures required in a primary nonoperational scenario to reconfigure the GR-unaware elements in the system. After the reconfiguration is complete, the elements can communicate with the secondary System Manager server to receive management or configuration information. This document also describes the functioning of GR-unaware elements with System Manager in general and the secondary System Manager server in particular.

**\* Note:**

The system does not replicate the `/etc/hosts` file of the primary System Manager server to the secondary System Manager server. If you have elements that depend on the entries present in the `/etc/hosts` file of the primary server, you must make the appropriate entries during the failover process.

**Related links**

[Geographic Redundancy terminology](#) on page 98

## Elements Geographic Redundancy manageability status matrix

The following table provides the status of managing the elements in the Geographic Redundancy setup from System Manager:

| Element                                      | Version         | Geographic Redundancy-enable status |
|----------------------------------------------|-----------------|-------------------------------------|
| Avaya Aura® Session Manager                  | 6.3 and later   | GR-aware (Auto)                     |
|                                              | 6.2 and earlier | GR-unaware                          |
| Communication Manager                        | 6.2 and earlier | GR-aware (Manual)                   |
| CS 1000                                      | 7.5             | GR-aware                            |
| Visualization, Performance and Fault Manager | 3.0             | GR-aware                            |
| Avaya Aura® Contact Center                   | 6.3             | GR-aware                            |
| Avaya Breeze® platform                       | 3.0             | GR-aware                            |

*Table continues...*

| Element                                                                                                                                                          | Version | Geographic Redundancy-enable status |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------------------------------|
| For information about the Geographic Redundancy terminology, see the “Geographic Redundancy terminology” section.                                                |         |                                     |
|  <b>Note:</b><br>The elements that are not listed in this table are GR-unaware. |         |                                     |

## Configuring various elements to change to the secondary System Manager

### Introduction

The sections describe how to reconfigure various GR-unaware elements that the secondary System Manager server manages when the server is activated during outages for an extended period of time, typically for more than 4 hours.

For outages that are less than 4 hours and that occur due to a primary System Manager server failure or a partial network breakdown, do not activate the secondary System Manager server.

If you perform the failover, the recovery process might take a few hours, depending on the data size and whether the recovery is done using the primary or secondary System Manager data.

### Session Manager configuration

Session Manager Release 6.3 and later elements are GR-aware.

In the normal operation mode, all Session Manager Release 6.3 and later elements communicate with the primary System Manager server for provisioned and configuration data.

You can configure both the primary and the secondary System Manager servers as unique trap destinations on each element. During a failover, the primary System Manager server becomes nonoperational, and you must manually activate the secondary System Manager server. Subsequently, all Geographic Redundancy-aware Session Manager elements automatically switch to the secondary System Manager server by using the Arbiter process of Session Manager.

In the primary nonoperational mode, each Session Manager element continues to interact with the primary System Manager server until the element receives an Activation notification from the secondary System Manager server. After the Session Manager element receives a secondary Activation notification, the element switches to the primary nonoperational mode.

In the primary nonoperational mode, the Session Manager element continuously polls the two System Manager servers to determine the current states.

Session Manager continues to communicate with the current managing System Manager server until there is a network disconnect or fragmentation. If there is a disconnect, for example, because

of a network split, the Session Manager switches to an active System Manager that is reachable within the network.

 **Note:**

From the web console of the active System Manager, you can override the automatic switching of Session Manager by using the Manage option.

Session Manager support only Manage operation. These elements do not support the Geographic Redundancy UnManage operation.

**Related links**

[Configuring Session Manager Release 6.2 and earlier during GR failover](#) on page 134

[Configuring Session Manager Release 6.2 and earlier during failback](#) on page 134

[Problems in managing Session Manager 6.1 or 6.2 using System Manager 6.2](#) on page 135

## Configuring Session Manager Release 6.2 and earlier during GR failover

Session Manager 6.2 or earlier releases are GR-unaware elements.

### About this task

During a failover, perform this procedure to configure the Session Manager elements to switch to the activated secondary System Manager server:

### Procedure

1. Log in to Session Manager as `cust` or `service`.
2. Run the `ChangeManagementIP` script with the secondary System Manager IP address or FQDN as the target.
3. Stop Session Manager.

Session Manager registers as a DRS node with the secondary System Manager server.

4. Start Session Manager.

The Session Manager element is marked for repair and gets DRS initial load from the secondary System Manager server.

The system overwrites the existing data of the element with the current data in the secondary System Manager database.

**Related links**

[Session Manager configuration](#) on page 133

## Configuring Session Manager Release 6.2 and earlier during failback

During the failback when the primary System Manager server is back online after an outage or failure and ready to serve the devices, you must perform the restore operation. During the restore operation, you can retain the primary or the secondary System Manager database.



## About this task

### Caution:

The following procedure impairs service. Therefore, schedule the restore operation outside of service hours.

When the primary System Manager server is functional, use this procedure to switch back the System Manager elements earlier than Release 6.3 to the primary System Manager server and resume normal operation.

## Procedure

1. Log in to Session Manager as `cust` or `service`.
2. At the prompt, perform the following:
  - a. Enter `cd /opt/Avaya/bin`.
  - b. Enter `ChangeManagementIP` and provide the IP address or FQDN of the secondary System Manager server as the target.

The command changes the configuration on the element. The system prompts for the enrollment password of the primary System Manager server.

3. Stop Session Manager.

Session Manager registers as a DRS node with the primary System Manager server.

4. Start Session Manager.

The Session Manager element is marked for repair and gets DRS initial load from the primary System Manager server.

The system overwrites the existing data of the element with the current data in the primary System Manager server.

## Next steps

After the recovery operation is complete, enable the Geographic Redundancy replication on System Manager web console.

## Related links

[Session Manager configuration](#) on page 133

## Problems in managing Session Manager 6.1 or 6.2 using System Manager 6.2

Do not manage Session Manager 6.2 or 6.1 using System Manager 6.2. If you deploy SIP Endpoints, ensure that this configuration is not a long-term configuration as some functionality is lost in the configuration.

Users cannot successfully complete certain Personal Profile Manager (PPM) operations if the SIP phone is registered to a System Manager 6.1 or 6.2 that is getting service from System Manager 6.3. For example:

- Add a contact to the contact list.

- Update a contact on the contact list.
- Delete a contact from the contact list.
- Change and save the phone volume settings.
- Change and save specific phone settings using the **Home > Settings** menu on the phone, for example, from the 96x1 SIP phone.
- Save the phone identity and update the time of the latest PPM login in the database.

The system internally saves the phone settings and the volume settings operations in the phone, but the settings are lost when you reboot the phone. To retain the settings, the user must log out and log in again. Ensure that another user does not log in to the same phone before the original user logs in back.

#### Related links

[Session Manager configuration](#) on page 133

---

## Communication Manager configuration

### Configuring Communication Manager during GR failover

Communication Manager is GR-unaware, regardless of the software release.

#### About this task

When the primary System Manager server has failed and the secondary System Manager server is activated, the replication is disabled.

Perform this procedure to configure the Communication Manager elements to switch to the secondary System Manager server.

#### Procedure

1. Log on to the web console of the secondary System Manager server.
2. In the left navigation pane, click **Services > Inventory > Manage Elements**. The system displays the status of Communication Manager as Unmanaged. You cannot administer the Communication Manager elements that System Manager does not manage.
3. Select the Communication Manager elements that you can manage or administer.
4. Click **More Actions > Manage**.
5. Click **Inventory > Synchronization > Communication Manager**.
6. Select the newly managed Communication Manager elements.

Ensure that the system displays the Communication Manager state as Managed.

7. Select Initialize data for selected devices, and click **Now**.

The secondary System Manager server retrieves all data from Communication Manager and is now ready to administer and manage Communication Manager.

 **Note:**

You must perform the Communication Manager synchronization only if Communication Manager is not synchronized with the secondary System Manager server, which happens if the secondary System Manager server is not synchronized with the primary server due to a split network. If you are unsure whether Communication Manager is synchronized with the current System Manager, follow the Synchronization steps.

## Configuring Communication Manager during GR failback

### About this task

Perform the Geographic Redundancy failback operation to resume normal operational behavior.

### Procedure

1. Log on to the web console of the primary System Manager server.
2. Deactivate the secondary System Manager server.

In this state, the heartbeat mechanism between the primary and secondary System Manager servers resumes as in a normal operation scenario, but the Geographic Redundancy replication between the System Manager servers is disabled.

3. Perform the recovery operation and retain the primary or the secondary database of System Manager. During recovery, you can select one of the following databases:
  - The database of the primary System Manager server.
    - The primary System Manager server resumes the state that the server was in before becoming nonfunctional.
    - You cannot see the administration that is performed while the secondary System Manager server manages the devices on the primary System Manager server. Inconsistency in data between Communication Manager and the primary System Manager database is likely. Therefore, run the initialize data job of Communication Manager. If you fail to initialize data, the data between Communication Manager and the primary System Manager server remains inconsistent.
  - The database of the secondary System Manager server.
    - The system overwrites the data in the primary System Manager server.
    - The system restores all the administration or changes done while the secondary server was serving the devices to the primary System Manager server.
    - The primary System Manager server displays the status of all Communication Manager servers that the secondary System Manager manages as UnManaged.

To manage the Communication Manager servers, navigate to **Home > Services > Inventory > Manage Elements** on the primary System Manager server and click **More Actions > Manage**.

### Next steps

Enable the Geographic Redundancy replication on System Manager web console.

## Communication Manager configuration when the primary System Manager server is nonoperational

In the primary nonoperational scenario, you might reach some of the Communication Manager elements from only one of System Manager servers.

## Configuring Communication Manager during GR failover when only the primary server is reachable

### About this task

Communication Manager Release 6.2 and later have a feature to notify all the changes made outside System Manager, for example, using Communication Manager, System Administration Terminal to the configured System Manager. To leverage the notify feature in System Manager Geographic Redundancy, configure Communication Manager with the IP addresses of the primary and the secondary System Manager server in the notification list.

For Communication Manager elements that you can reach only from the secondary System Manager server, perform the following procedure to configure Communication Manager elements to change to the secondary System Manager server.

During failback, perform the same procedure by reversing the roles of the primary and secondary System Manager servers.

### Procedure

1. Log on to the web console of the primary System Manager server.
2. In the left navigation pane, click **Services > Inventory > Manage Elements**.

The system displays the status of Communication Manager as Unmanaged. You cannot administer Communication Manager elements that System Manager does not manage.

3. Select Communication Manager elements that the secondary System Manager server must manage.
4. Click **More Actions > Manage**.

5. Log on to the web console of the secondary System Manager server.

6. In the left navigation pane, click **Services > Inventory > Manage Elements**.

The system displays the status of Communication Manager as Unmanaged. You cannot administer the Communication Manager elements that System Manager does not manage.

7. Select Communication Manager elements that you must change to the secondary System Manager server.
8. Click **More Actions > Manage**.

9. Click **Inventory > Synchronization > Communication Manager**.

Perform Step 10 only if Communication Manager is not synchronized with the secondary System Manager server. This can happen if the secondary System Manager server is not synchronized with the primary System Manager server due to reasons such as the nonoperational state of the primary or split network.

10. Select the newly managed Communication Manager elements.

Ensure that the system displays the manageability status of Communication Manager as Managed.

11. Select Initialize data for selected devices, and click **Now**.

The secondary System Manager server retrieves all data from Communication Manager and is now ready to administer and manage Communication Manager.

 **Note:**

To find the difference between data on the primary and secondary System Manager servers during failback, use **Services > Geographic Redundancy > Restore Data**. The Restore Data dialog box displays comparative data between the primary and secondary System Manager servers when the primary System Manager server is nonoperational. This includes the number of elements that were managed by the primary and secondary System Manager servers, the number of entities modified on the primary and secondary System Manager servers, and the link to the audit logs. With the comparative data, you can decide whether to use secondary or primary System Manager data during failback.

---

## CS 1000 configuration

CS 1000 elements are Active-Active GR-aware. The GR-aware CS 1000 elements are configured to interact with both primary and secondary System Manager servers. The element communicates with System Manager servers for Authentication and Authorization (A&A) related operations. Typically, the element leverages A&A services from the System Manager server that is closest to the element regardless of whether the server is in the primary or secondary mode. The secondary System Manager can serve A&A requests in both standby and active modes.

CS 1000 server deployments are of two types:

- VxWorks-based servers
- Linux-based servers

### Related links

[Configuring CS 1000 SNMP alarms](#) on page 139

[Configuring VxWorks-based CS 1000 servers](#) on page 140

[Configuring Linux-based CS 1000 servers](#) on page 140

[Limitations to the CS 1000 functionality support on System Manager](#) on page 142

## Configuring CS 1000 SNMP alarms

### Procedure

1. Get the port number for the CS 1000 SNMP profile.

For more information, see TrapListener service. The default port is 10162.

2. Configure CS 1000 SNMP alarms on the CS 1000 element by using the port number that you received.

For more information, see *Fault Management - SNMP Avaya Communication Server 1000*, NN43001-719.

3. Manage alarms on System Manager.

For more information, see Manage alarms.

#### Related links

[CS 1000 configuration](#) on page 139

[Alarming](#) on page 990

[TrapListener service](#) on page 1030

## Configuring VxWorks-based CS 1000 servers

### Procedure

Run the following commands to register the information on CS 1000 servers:

```
Register UCMSecurity System
join secDomain
```

#### Related links

[CS 1000 configuration](#) on page 139

## Configuring Linux-based CS 1000 servers

System Manager Geographic Redundancy deployment does not support some of the CS 1000 functionality. For more information, see Limitations to the CS 1000 functionality support on System Manager.

### Procedure

1. On the Security Configuration page, click **Full security configuration** and **Security Configuration**.

The system displays the FQDN validation page.

2. Confirm that the (TLAN) IP address and FQDN values are correct, and click **Next**.

The system displays the Select server type page.

3. Click **Member server** and click **Next**.

The system displays the Enter server information page.

4. Enter the (TLAN) IP address of the primary security server, and click **Next**.

The system displays the Verify primary security server fingerprint page.

5. Verify that the FQDN and fingerprint information for the primary security server is valid, and enter the following details in appropriate fields:

- The primary security server user ID, that is, a UCM user ID with System Administrator role.

- The primary security server password of the user.
6. Click **Next**.  
The system displays the Enter certificate information page.
  7. Enter information in appropriate fields.
  8. Click **Finish**.  
The system displays the Security Configuration Progress page.
  9. To complete the configuration process, click **Restart**. to restart the web server.  
The Security Configuration Progress page confirms that the server is restarting.  
  
The restart process might take up to 5 minutes to complete. You can then establish a new session and log on with your security administrator credentials. The registration process requires configuration of the primary System Manager information on the element. The secondary server information is provided to the element when the element registers with the primary server.

#### Related links

[CS 1000 configuration](#) on page 139

## Limitations to the CS 1000 functionality support on System Manager

| System Manager server state                 |                  | CS 1000 functionality support available                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                              |
|---------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary server                              | Secondary server | From the primary server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | From the secondary server                                                                                                                                                                                                                    |
| Active, reachable from the secondary server | Standby          | <ul style="list-style-type: none"> <li>• Authentication (SSO)</li> <li>• Authorization (RBAC)</li> <li>• Trust Management</li> <li>• Starting of Remote Element Managers</li> <li>• Alarm Management (Display CS 1000 alarms)</li> <li>• Log Harvesting</li> <li>• Audit Log Collection</li> <li>• IPsec Manager</li> <li>• SNMP Manager</li> <li>• Corporate Directory</li> <li>• Registration of the new CS 1000 member</li> <li>• User Management of CS 1000 elements</li> <li>• Starting of Deployment Manager</li> <li>• Starting of Patch Manager</li> </ul> | <ul style="list-style-type: none"> <li>• Authentication (SSO)</li> <li>• Authorization (RBAC)</li> <li>• Starting of Remote Element Managers</li> </ul>                                                                                      |
| Nonoperational                              | Standby          | The primary server is non-operational. Therefore, no functionality is available from the primary server.                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• Authentication (SSO)</li> <li>• Authorization (RBAC)</li> <li>• Starting of Remote Element Managers</li> </ul>                                                                                      |
| Nonoperational                              | Active           | The primary server is non-operational. Therefore, no functionality is available from the primary server.                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• Authentication (SSO)</li> <li>• Authorization (RBAC)</li> <li>• Starting of Remote Element Managers</li> <li>• Alarm Management (Display CS 1000 Alarms)</li> <li>• Audit Log Collection</li> </ul> |

### Related links

[CS 1000 configuration](#) on page 139



---

## Meeting Exchange configuration

Meeting Exchange elements are GR-unaware. All communications except for WebLM are initiated from System Manager to Meeting Exchange. For licensing, a WebLM client on Meeting Exchange initiates communication with System Manager. For Meeting Exchange configuration, the data on System Manager is stored in the form of a Binary Large Object (BLOB) and synchronized with the element by using a scheduler job that runs every minute. The Meeting Exchange element is registered with System Manager. As these entities are replicated from the primary to the secondary server, information about the Meeting Exchange elements is present with the secondary System Manager server as well. You do not have to explicitly establish trust between the Meeting Exchange element and System Manager.

### Related links

[Element configuration](#) on page 143

[License management](#) on page 143

## Element configuration

In the failover scenario, you can perform all Meeting Exchange configuration changes from the activate secondary System Manager server. The system synchronizes the changes with the Meeting Exchange element by using Scheduler job. You do not require to make changes on the Meeting Exchange element in this case.

### Related links

[Meeting Exchange configuration](#) on page 143

## License management

To provision licensing from the secondary server, reassociate the Meeting Exchange element with the secondary server. To reassociate the Meeting Exchange element, remove the Meeting Exchange entry from **Services > Inventory > Manage Elements** of the secondary System Manager server and add the entry back again.

### Related links

[Meeting Exchange configuration](#) on page 143

---

## Presence Server configuration

Presence Server 6.2.x and earlier elements are GR-unaware. During failover, configure the Presence Server elements manually to switch to the secondary System Manager. Presence Server elements are registered in System Manager from **Services > Inventory**. All Presence Server configuration data is replicated from the primary to the secondary System Manager server.

### Related links

[Configuring Presence Server](#) on page 144

## Configuring Presence Server

### About this task

Perform this procedure to switch Presence Server elements to the secondary server:

### Procedure

1. Create a backup of the Presence Server data after the failover to be invoked manually by an operator after the failover of System Manager.
2. Run the `changeSMGRFQDN.sh` script on Presence Server element to change Presence Server System Manager configuration from the primary System Manager to secondary System Manager.

The script changes all configurations on the Presence Server element but does not affect Presence Server entries or configuration on System Manager. Presence Server calls InitTM to establish trust with the secondary System Manager. The element is re-registered on the secondary System Manager. The element is registered in DRS and **Services > Inventory**. As part of the registration, Presence Server element is added in `/etc/hosts` of the secondary System Manager. DRS marks the element for repair and sends the initial load of data to the element. Data on System Manager overwrites data on Presence Server element.

3. Log out or log in to the endpoints on failover.
4. Create a backup of Presence Server element after System Manager failover to ensure that the new configuration data is backed up.
5. To ensure continued serviceability support during primary nonoperational scenarios, configure Presence Server elements with both the primary and secondary System Manager servers as trap destinations.

For instructions to configure trap destinations on Presence Server element, see *Administering Avaya Aura® Presence Services*.

### Related links

[Presence Server configuration](#) on page 143

---

## Messaging configuration

Messaging elements are GR-unaware. However, the Messaging element manager is GR-aware. Messaging includes Avaya Aura® Messaging, Modular Messaging, and Communication Manager Messaging.

### Related links

[Configuring Messaging in the normal operational mode](#) on page 145

[Configuring Messaging when the primary System Manager server is nonoperational](#) on page 145

[Configuring Messaging during GR fallback](#) on page 146

[Configuring Messaging during split network](#) on page 147

## Configuring Messaging in the normal operational mode

### Before you begin

- Add both the primary and secondary servers as Trusted Servers in the Messaging system.
- Update the **Login**, **Password**, and **Confirm Password** fields with the appropriate trusted server defined on the Messaging system.

### Procedure

1. Log on to the primary System Manager server.
2. On the System Manager web console, click **Services > Inventory**.
3. In the navigation pane, click **Manage Elements**.
4. On the Manage Elements page, click **New** and add the Messaging system.
5. Provide the name and IP address of the Messaging system.
6. On the **Attributes** tab, fill the **Login**, **Password**, and **Confirm Password** fields with the corresponding name and password of the Messaging trusted server.
7. Click **Inventory > Synchronization > Messaging System**. Select the required Messaging element, and click **Now**.
8. Perform one of the following:
  - If synchronization is successful, perform the administration task on Messaging.
  - If synchronization fails, check the login details for Messaging.
9. Log on to the secondary System Manager server.
10. On the System Manager web console, click **Services > Inventory**.
11. In the navigation pane, click **Manage Elements**.
12. Ensure that the Messaging system that has been added is visible on the Manage Elements page.

### Related links

[Messaging configuration](#) on page 144

## Configuring Messaging when the primary System Manager server is nonoperational

Perform this procedure to switch the Messaging system to the secondary System Manager when the primary System Manager server fails.

### Before you begin

- Add both the primary and secondary servers as Trusted Servers in the Messaging system.
- Update the **Login**, **Password**, and **Confirm Password** fields with the appropriate trusted server defined on the Messaging system.

## Procedure

1. Log on to the Messaging system that System Manager manages.
2. Add the secondary System Manager server as Trusted Servers in the Messaging system.
3. Log on to the secondary System Manager server.
4. On the System Manager web console, click **Services > Inventory**.
5. In the navigation pane, click **Manage Elements**.
6. On the Manage Elements page, select the Messaging system that you want to change to the secondary System Manager server.
7. Click **Edit**.
8. On the **Attributes** tab, fill the **Login**, **Password**, and **Confirm Password** fields with the corresponding name and password of the Messaging trusted server.
9. Click **Commit**.
10. Click **Inventory > Synchronization > Messaging System**, and select the required Messaging element.
11. Click **Now**.

The secondary System Manager server retrieves all data from Messaging and is now ready to administer and manage Messaging.

## Related links

[Messaging configuration](#) on page 144

## Configuring Messaging during GR failback

### Before you begin

Complete the GR failback from the database of the primary System Manager server.

## Procedure

1. Log on to the primary System Manager server.  
If the trusted server entry for the primary System Manager server is already present in Messaging, perform from the Step 3 e.
2. **(Optional)** Remove the secondary System Manager server as the trusted server in the Messaging system.
3. If you select the database of the secondary System Manager server to recover the data, perform the following steps:
  - a. On the web console of the primary System Manager server, click **Services > Inventory**.
  - b. In the left navigation pane, click **Manage Elements**.
  - c. Select the Messaging element that you must change to the primary System Manager server.

- d. Click **Edit**.
- e. On the Manage Elements page, navigate to the **Attributes** tab and update the **Login**, **Password**, and **Confirm Password** fields with the corresponding name and password of the Messaging trusted service.
- f. Click **Commit** to apply the changes.
- g. Click **Inventory > Synchronization > Messaging System**.
- h. Select the required Messaging element, and click **Now**.

The primary System Manager server retrieves all data from Messaging and is now ready to administer and manage Messaging.

#### Related links

[Messaging configuration](#) on page 144

## Configuring Messaging during split network

### About this task

Do not activate primary and secondary System Manager servers except during scenarios such as the primary System Manager server is nonoperational. When the primary System Manager server is nonoperational, not all elements are reachable from either System Manager servers.

Perform the procedure on the primary System Manager server. You cannot administer Messaging on the secondary System Manager server in the standby mode.

### Procedure

1. Log on to the primary System Manager server and the System Manager server and verify that the system displays the replication status as disabled.
2. Add System Manager as the trusted server in the Messaging system.  
If the server is already added as the trusted server, update the login and password details of Messaging for both System Manager servers.
3. Click **Services > Inventory**.
4. In the left navigation pane, click **Synchronization > Messaging System**.
5. Select the Messaging element and click **Now**.
6. Perform one of the following:
  - If the synchronization is successful on both System Manager servers, perform the administration task for Messaging on both System Manager servers.
  - If the synchronization fails, check the login details for Messaging.

While performing administrative tasks on Messaging, the system displays a warning message that the changes can result data inconsistency.
7. To perform administration tasks only on the primary System Manager server, remove the trusted server entry of the secondary System Manager server from Messaging.

## Related links

[Messaging configuration](#) on page 144

---

## Avaya Aura® Conferencing configuration

Avaya Aura® Conferencing elements are GR-unaware. During a failover or split network, you must manually configure to point the Avaya Aura® Conferencing element to the secondary System Manager server.

The following components of Avaya Aura® Conferencing are integrated with System Manager:

- License Management
- Trust Management
- User Management
- Logs
- Single Sign-On
- Role based access control
- Alarms

## Related links

[Configuring Avaya Aura Conferencing to be managed by System Manager](#) on page 148

[License management](#) on page 150

[Trust management](#) on page 150

[Single Sign-On and Role Based Access Control](#) on page 150

[User management](#) on page 151

[Logs](#) on page 151

[Alarms](#) on page 151

## Configuring Avaya Aura® Conferencing to be managed by System Manager

### Before you begin

From System Manager, get the information for the community string and the Trap Listener port number.

### About this task

For the Avaya Aura® Conferencing components to function, configure the IP address and FQDN of the active System Manager in the Element Manager console of Avaya Aura® Conferencing.

### Procedure

1. On the web browser, type `http://<IP address>:12120`.

where *IP address* is the logical IP address of the server that is running the Element Manager Internal OAM Service.

2. Press **Enter**.

The system displays a webpage with the IP address that you entered and the **Launch Element Manager Console** link.

3. Click **Launch Element Manager Console**.
4. In the navigation pane of **Element Manager Console**, select **Addresses**.
5. In the Addresses window, click **Add (+)**.
6. In the Add IPv4 Address dialog box, complete the following fields:
  - **Logical Name**: Type SMGRAddress.
  - **IPv4 Address**: Type the IP address of the primary System Manager.
7. Click **Apply**.
8. Repeat Step 3 through Step 5 on the secondary System Manager, and enter a logical name and IP address.
9. In the navigation pane, click **External Nodes**.
10. In the External Nodes window, click **Add (+)**.
11. In the Add External Nodes dialog box, complete the following fields:
  - **Name**: Type SMGRNode.
  - **IPv4 Address**: Select SMGRAddress from the list.
12. Click **Apply**.
13. Repeat Step 8 through Step 10 for the secondary System Manager, and enter a name.  
Select the logical name that you entered in Step 6.
14. In the navigation pane, click **OAM Profiles > OSS Servers**.
15. Click **Add (+)**.
16. In the Add OSS Server dialog box, complete the following fields:
  - **Name**: Type a name, for example, SmgrOssServer.
  - **Node**: Select SmgrExtNode from the list.
  - **Use External OAM Network**: Do not select this check box.
17. Click **Apply**.
18. Repeat Step 12 through Step 15 for the secondary System Manager, and enter a name.  
Select the node entered in Step 11.
19. In the navigation pane, click **OAM Profiles > SNMP Managers**.
20. Click **Add (+)**.
21. In the Add SNMP Manager dialog box, complete the following fields:
  - **Name**: Type a name, for example, SmgrSnmpManager.

- **Community:** Type the community string as obtained from System Manager.
- **Servers:** Select the server name you created in Step 14, for example, SmgrOssServer.
- **Trap Port:** Type the Trap Listener port number as obtained from System Manager.

22. Click **Apply**.

23. Repeat Step 17 through Step 20 for the secondary System Manager, and enter a name, the community string, and the trap port.

Select the server name that you entered in Step 16.

24. Restart Element Manager through SSH to the server.

#### Related links

[Avaya Aura Conferencing configuration](#) on page 148

## License management

Avaya Aura® Conferencing license key is installed on System Manager for forwarding license requests to the Avaya WebLM server residing on System Manager. For initial setup with the primary or active System Manager, follow the procedure in *Deploying Avaya Aura® Conferencing*. During a failover in a System Manager Geographic Redundancy setup, for license management to work, reconfigure the IP address and FQDN to match the IP address and FQDN of the active System Manager.

#### Related links

[Avaya Aura Conferencing configuration](#) on page 148

## Trust management

For the initial setup, follow the procedures in *Deploying Avaya Aura® Conferencing*. Because the same root Certificate Authority exists on the primary and the secondary System Manager, you can use the same end-identity certificate for both System Manager servers. During a failover in a System Manager Geographic Redundancy setup, for trust management to work, reconfigure the IP address and FQDN to match the IP address and FQDN of the active System Manager.

#### Related links

[Avaya Aura Conferencing configuration](#) on page 148

## Single Sign-On and Role Based Access Control

For the initial setup, follow the procedures in *Deploying Avaya Aura® Conferencing*. In a System Manager Geographic Redundancy setup, all elements in the inventory, such as Avaya Aura® Conferencing Element Manager and Avaya Aura® Conferencing Provisioning Client, admin users and passwords, Role Based Access Control (RBAC) attributes replicate between the primary and secondary System Manager. For Single Sign-On (SSO) and RBAC to function during a failover, reconfigure the IP address and FQDN to the IP address and FQDN of the active System Manager.

#### Related links

[Avaya Aura Conferencing configuration](#) on page 148



## User management

For the initial setup, follow the procedures in *Deploying Avaya Aura® Conferencing*. In a System Manager Geographic Redundancy setup, all elements in the inventory, user profiles, and user data in the System Manager database replicate between the primary and secondary System Manager. During a failover in System Manager Geographic Redundancy setup, Single Sign-On or RBAC must work for user management. Reconfigure the IP address and FQDN to match with the IP address and FQDN of the active System Manager.

### Related links

[Avaya Aura Conferencing configuration](#) on page 148

## Logs

For the initial setup, follow the log forwarding procedures in *Deploying Avaya Aura® Conferencing*. In a System Manager Geographic Redundancy setup, send the logs to the active System Manager. In a GR-enabled System Manager pair, the enrollment password is the same for the primary and active System Manager servers. During a failover in a System Manager Geographic Redundancy setup, for log forwarding to the active System Manager, run the logAgent script again with the IP address or FQDN of the active System Manager, the same https System Manager port, and the same enrollment password.

### Related links

[Avaya Aura Conferencing configuration](#) on page 148

## Alarms

For the initial setup, follow the alarm forwarding procedures in *Deploying Avaya Aura® Conferencing*. You can configure Avaya Aura® Conferencing to use two SNMP managers and hence two alarm destinations. See section 5.8.2 for configuring primary and secondary System Manager servers as two trap destinations.

### Related links

[Avaya Aura Conferencing configuration](#) on page 148

---

## Avaya Meetings Server configuration

The Avaya Meetings Server element is GR-unaware. During a failover or split network, you must manually configure SSO on the Avaya Meetings Management console.

### Note:

If secondary System Manager is using the same IP or FQDN of the primary System Manager, then you do not need to configure SSO for Avaya Meetings Server.

## Configuring SSO for Equinox Conferencing

### Exchanging CA certificates between System Manager and Avaya Meetings Management

#### About this task

If the Avaya Meetings Management CA certificate is not issued by the System Manager CA, perform the following.

#### Procedure

1. Download the CA PEM file from System Manager.

For more information, see “Downloading the System Manager PEM certificate”.

#### **Note:**

If System Manager has more than one CA, import all the CAs into Avaya Meetings Management.

2. Log in to the Avaya Meetings Management administrator portal.
3. To import the CA PEM file into Avaya Meetings Management, click **Settings > Security > Certificate**.
4. Click **Import**.
5. On the Import certificates dialog box, click **Add** to select the downloaded PEM file, and click **Apply**.
6. Restart Avaya Meetings Management.
7. To download the Avaya Meetings Management CA certificate, click **Settings > Security > Certificate**.
8. On the Certificates page, click **Conferencing Management Certificate**.
9. On the System Manager web console, click **Services > Inventory**.
10. In the navigation pane, click **Manage Elements**.
11. On the Manage Elements page, select the System Manager certificate and click **More Actions > Manage Trusted Certificates**.
12. On the Manage Trusted Certificates page, click **Add**.
13. On the Add Trusted Certificates page, click **Import as PEM certificate**.
14. Copy the content of the Avaya Meetings Management CA certificate and paste the content in the text box provided on the Add Trusted Certificates page.
15. Click **Commit**.

#### Related links

[Avaya Meetings Server configuration](#) on page 151

[Downloading the System Manager PEM certificate](#) on page 153

[Configuring SSO in Avaya Meetings Management](#) on page 153

**Downloading the System Manager PEM certificate****Procedure**

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > CA Structure & CRLs**.
4. Click **Download PEM file**.

The system downloads the .pem file on your system.

**Related links**

[Exchanging CA certificates between System Manager and Avaya Meetings Management](#) on page 152

**Configuring SSO in Avaya Meetings Management****Before you begin**

If the Avaya Meetings Management CA certificate is not issued by the System Manager CA, exchange CA certificates between Avaya Meetings Management and System Manager.

- Download the CA certificate from System Manager and import the certificate into the Avaya Meetings Management console.
- Download the certificate from the Avaya Meetings Management console and add the certificate in to System Manager as a new trusted certificate.

For more information, see “Exchanging CA certificates between System Manager and Avaya Equinox Management”.

**Procedure**

1. Navigate to `/opt/Avaya/iview/tomcat/webapps/iview/WEB-INF/classes/sso_config/securityServerConfig.properties`, and edit the properties of the file as follows.

```
openssoclient.config.folder=../config
com.iplanet.am.cookie.name=<FQDN of your System Manager>
security.server.fqdn=<FQDN of your System Manager>
```

2. Navigate to `/opt/Avaya/iview/tomcat/config/vcs-core.properties` and add the `vnex.auth.smgr.sso=true` property.
3. Before restarting Tomcat, navigate to `/opt/Avaya/iview/tomcat/config/` and delete the `OpenSSOClient` folder.
4. To restart Tomcat, do one of the following:
  - On the shell, run the `service avaya.iview restart` command.
  - On the Avaya Meetings Management console, click **Restart**.

**Related links**

[Avaya Meetings Server configuration](#) on page 151

[Exchanging CA certificates between System Manager and Avaya Meetings Management](#) on page 152

---

## IP Office configuration

IP Office elements are GR-unaware. During failover, split network, or failback, perform the procedures from this section to ensure data integrity and proper administration of IP Office from System Manager. As the System Manager certificates contain an entry of the secondary System Manager in the **SAN** field, the same trust continues to work between the secondary System Manager and the IP Office element.

### Important:

- The System Manager lock is maintained on the IP Office device to ensure that changes are not provisioned on the device outside System Manager. You can only make configuration changes on IP Office after removing the System Manager lock. For more information, see *Implementing IP Office*.
- If IP Office has been added to any System Manager previously, then before reusing it, you must erase the IP Office security settings using the **File > Advanced > Erase Security Settings** page on the IP Office Manager window.

### Related links

[Configuring IP Office in normal operational mode with SCEP enabled](#) on page 154

[Configuring IP Office in normal operational mode with SCEP disabled](#) on page 155

[IP Office configuration when the primary System Manager is nonfunctional](#) on page 156

[IP Office configuration in the Active-Active scenario](#) on page 156

[Alarms](#) on page 156

[User management](#) on page 156

## Configuring IP Office in normal operational mode with SCEP enabled

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **RA Functions > Add End Entity** and add IP Office as an entity and specify all required details.
4. On the IP Office device, open the security settings and perform the following:
  - a. Set SCEP to **active**.
  - b. Specify the correct IP address of System Manager and the certificate name that you added on System Manager.
  - c. Set the received certificates check to **High**.
5. Log on to the web console of the primary System Manager server.

6. On the System Manager web console, click **Services > Inventory**.
7. In the navigation pane, click **Manage Elements**.
8. Click **New**.
9. On the Add IP Office page, provide the name, the IP address, and the valid user name and password for IP Office.
10. Verify that the system receives the SCEP requests from the device at the specified interval using system monitor for the IP Office device.  
  
The primary System Manager server is now ready to administer and manage the IP Office device.
11. Log on to the web console of the secondary System Manager and click **Services > Inventory**.
12. In the left navigation pane, click **Manage Elements**.  
  
The Manage Elements page displays the IP Office devices that you added on the primary System Manager.

#### Related links

[IP Office configuration](#) on page 154

## Configuring IP Office in normal operational mode with SCEP disabled

### Procedure

1. Log on to the web console of the primary System Manager server.
2. On the System Manager web console, click **Services > Inventory**.
3. In the navigation pane, click **Manage Elements**.
4. Click **New**.
5. On the Add IP Office page, provide the name, the IP address, and the valid user name and password for IP Office.
6. Click **Commit**.  
  
The primary System Manager server is now ready to administer and manage the IP Office device.
7. Log on to the web console of the secondary System Manager, and click **Services > Inventory**.
8. In the left navigation pane, click **Manage Elements**.  
  
The Manage Elements page displays the IP Office devices that you added on the primary System Manager.

#### Related links

[IP Office configuration](#) on page 154

## IP Office configuration when the primary System Manager is nonfunctional

If the primary System Manager server is nonfunctional, the secondary System Manager server can administer and manage the IP Office device without any additional steps on the secondary System Manager.

### Related links

[IP Office configuration](#) on page 154

## IP Office configuration in the Active-Active scenario

If the primary System Manager server is nonfunctional, the secondary System Manager server can administer and manage the IP Office device without any additional steps on the secondary System Manager.

If the IP Office element can communicate with both System Manager servers, you can administer IP Office from both System Manager servers. The data from the two servers conflict. During recovery, you must select the database of only one System Manager, and the changes in the other database are lost.

Manage the IP Office elements from only one System Manager even in the Active-Active scenario so that you can select this database for recovery when the communication between the two System Manager servers is reestablished. For more information about managing IP Office from System Manager, see *Implementing the Avaya IP Office for an Aura Configuration*.

### **Note:**

For configuring the trap destination, SCEP details, and WebLM server in a single step, run the Initial Installation Utility of Native B5800 Manager.

You can also use the installation utility to change the configuration on IP Office for the System Manager failover scenarios. As the System Manager certificates contain an entry of the secondary System Manager in the **SAN** field, the same trust continues to work between the secondary System Manager and IP Office.

### Related links

[IP Office configuration](#) on page 154

## Alarms

To ensure serviceability support in primary System Manager nonoperational scenarios, forward the alarms or traps from the IP Office elements to both the primary and secondary System Manager servers. Configure the IP Office device with IPs of both primary and secondary System Manager servers as a trap destination.

### Related links

[IP Office configuration](#) on page 154

## User management

IP Office elements are registered with System Manager in **Inventory > Manage Elements**. The inventory data is replicated from the primary System Manager to the secondary System Manager.

When the secondary System Manager server is activated after failover, you can use the IP Office element for user provisioning from the secondary System Manager without any changes to the IP Office device.

**Related links**

[IP Office configuration](#) on page 154

---

## Visualization, Performance, and Fault Manager

Visualization, Performance, and Fault Manager (VPFM) is Active-Active Geographic Redundancy-aware. VPFM is configured to communicate with primary and secondary System Manager servers. VPFM communicates with System Manager servers for Authentication and Authorization (A&A) operations, such as SSO and RBAC. Usually, the element leverages A&A services from the System Manager server which is closest to the element regardless of whether the server is in the primary or the secondary mode. The secondary System Manager can serve A&A requests in both the standby and active modes.

VPFM leverages System Manager for Common Service Client (SMGR-CS Client) that provides adopters with off-box SSO and RBAC solution that works with System Manager.

---

## Application Enablement Services

Application Enablement Services (AES) uses the licensing feature of System Manager. When System Manager fails, you must reconfigure the WebLM client on AES to point to the correct System Manager for using Licensing Service.

You can configure AES to integrate with centralized System Manager WebLM.

---

## Avaya Aura® Contact Center

Avaya Aura® Contact Center (AACC) is Active-Active GR-aware. AACC elements are configured to communicate with primary and secondary System Manager servers. The element communicates with System Manager servers for Authentication and Authorization (A&A) operations such as Single Sign-On (SSO) and Role Based Access Control (RBAC). Usually, the element leverages A&A services from the System Manager server that is closest to the element regardless of whether System Manager is in the primary or the secondary mode. The secondary System Manager can serve A&A requests in the standby and active modes.

---

## Avaya Multimedia Messaging configuration

Avaya Multimedia Messaging is GR-unaware. During the failover of the primary System Manager, you must configure the Avaya Multimedia Messaging server manually to use the secondary System Manager server.

For procedures to configure the System Manager connection details on the Avaya Multimedia Messaging server, see *Deploying Avaya Multimedia Messaging*. The document is available on the support site at <https://support.avaya.com>.



# Chapter 5: Managing groups and roles for resources

---

## Managing groups

---

### Group management

Group and Lookup Service (GLS) is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, changing, searching, and deleting groups and group memberships. Use GLS to group resources in ways that work best for the business, such as organizing resources by location, organization, and function.

On the System Manager web console, with GLS, you can assign different roles to administrators and allow administrators to perform only limited tasks on group of resources. For example, you can create a user group so that only an authorized user can manage the user group.

GLS supports group administration for the following common resources:

- Shared across elements, such as roles and users
- Unshared element-specific resources

GLS contains a repository of groups and memberships from System Manager and other applications that use the GLS service. GLS synchronizes the resources with other Avaya applications and services that manage these resources. GLS maintains resource IDs and their group memberships. With GLS, you can search for one or more resources based on their attribute values and get resource attributes for one or more resources.

With GLS, you can perform the following operations:

- Create groups.
- View and change groups.
- Create duplicate groups by copying properties of existing groups.
- Move groups across hierarchies.
- Assign and remove resources for groups.
- Delete groups.
- Synchronize groups.

As a shared service, GLS reduces the time and effort involved by defining reusable groups of managed resources that more than one application or service requires. For example, you can use the group of resources to assign permissions through Role Based Access Control (RBAC).

---

## Viewing groups

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, select a group and perform one of the following:
  - If the group is a selection-based group, click **View**.
  - If the group is a query-based group, click **View** and click **Execute Query**.

The system displays the View Group page with the details of the group and the resources assigned to the group.

### Related links

[View Group field descriptions](#) on page 170

---

## Creating groups

### About this task

You can create up to 300 groups.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, perform one of the following:
  - Click **New** to create a group.
  - Select a group and click **New** to create a subgroup within a group.
4. On the New Group page, enter the name, type, group membership, and a description of the group.
5. Click **Commit**.

The system creates the new group.

### Related links

[New Group field descriptions](#) on page 168

---

## Modifying groups

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, select a group.
4. Click **Edit** or **View > Edit**.
5. On the Edit Group page, enter the appropriate information.
6. Click **Commit** to save the changes to the database.

### Related links

[Edit Group field descriptions](#) on page 172

---

## Creating duplicate groups

### About this task

You can create a duplicate group by copying the properties of an existing group. When you create a duplicate group, the system copies all the information, except the hierarchy, from the existing group to the new group.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, select a group.
4. Click **Duplicate**.
5. On the Duplicate Group page, perform one of the following:
  - Click **Root** to create a duplicate group at the root level.
  - Select a group and click **Selected Group** to create a duplicate group within another group.

The system displays a copy of the parent group on the Group Management page.

6. Click the plus sign (+) to view the subgroups in a group.

### Related links

[Duplicate Group field descriptions](#) on page 174

---

## Deleting groups

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, select the groups that you want to delete.
4. Click **Delete**.
5. On the Delete Group confirmation page, click **Delete**.

The system confirms the successful deletion of groups and displays the details of groups that the system failed to delete.

The system does not delete the resources.

### Related links

[Delete Group Confirmation field descriptions](#) on page 173

---

## Moving groups

### About this task

You can move a group from one hierarchy to another.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, select a group.
4. Click **More Actions > Move**.
5. On the Move Group page, perform one of the following:
  - To move a group to the root level, click **Root**.
  - To move a group to a different group or subgroup, select the target group or subgroup, and click **Selected group**.
6. To view the subgroups in a group, click the plus sign (+).

### Related links

[Move Group field descriptions](#) on page 174

---

## Synchronizing resources for a resource type

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, click **More Actions > Sync**.
4. On the Resource Synchronization page, in the **Type** field, select the type of resources.
5. Click **Sync**.

### Related links

[Resource Synchronization field descriptions](#) on page 175

---

## Assigning resources to a group

### About this task

You can assign only resources of the type that is configured for the group. The type of resource that you can assign to a group is set when you create a group. For example, if the type of resource is set to Users, you can assign only user types to the group. If the type is set to ALL, you can assign all types of resource to the group.

#### **Note:**

In System Manager, the users that you add to a group can only manage the resources that are assigned to the group and cannot add new users.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, click **New**.
4. Enter the name of the group, and select a group type.
5. Perform one of the following:
  - To assign a resource to a new group, click **Assign Resources**.
  - To assign a resource to an existing group, perform one of the following:
    - Click **Edit > Assign Resources**.
    - Click **View > Edit > Assign Resources**.

6. On the Resources page, select a resource.

The Resources page displays all resources available in the application. You cannot select the resources that are assigned to a group.

You can also search for a resource by using **Advance Search**.

7. Click **Add To Group**.

The system adds the selected resources to the group.

**Related links**

[Resources field descriptions](#) on page 178

---

## Searching for resources

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the left navigation pane, perform one of the following:
  - Click **Groups**.
  - Click **Resources** and continue with Step 4.
3. On the Group Management page, perform one of the following:
  - Click **New > Assign Resources**.
  - Select a group and click **Edit > Assign Resources**.
  - Select a group and click **View > Edit > Assign Resources**.
4. On the Resources page, click **Advanced Search**.
5. In the **Criteria** area, perform the following:
  - a. In the **Type** field, select the resource type.
  - b. In the **Resource Attributes** area, select the attribute name, the matching operator, and the search string from the appropriate fields.
6. To add more than one search condition, click the plus sign (+).

Click the minus sign (-) to delete a search condition. You can delete a search condition only if you have more than one search condition.
7. In the drop-down field, click **And** or **Or**.

The system displays this option only when you use the plus sign (+) to add a search condition.
8. Click **Search**.

The **Resources** section displays the resources that match the search criteria. If no resources match the search criteria, the **Resource** section displays the message `No records are found`.

---

## Searching for groups

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, click **Advanced Search**.
4. In the **Resource Attributes** section, select the attribute name, the matching operator, and the search string from the appropriate fields.
5. To add more than one search condition, click the plus sign (+).  
Click the minus sign (-) to delete a search condition. You can delete a search condition only if you have more than one search condition.
6. In the drop-down field, select **And** or **Or**.

The system displays this option when you use the plus sign (+) to add a search condition.

7. Click **Search**.

### Related links

[Resources field descriptions](#) on page 178

---

## Filtering groups

### About this task

You can apply filter to the following fields:

- **Name**
- **Type**
- **Hierarchy**

You can filter groups by a single column or multiple columns.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. On the Group Management page, click **Filter: Enable**.
4. In the **Name** field, enter the group name.
5. In the **Type** field, select the resource type.
6. In the **Hierarchy** field, enter the hierarchy level.

When you enter a hierarchy level, the table displays only those groups that you created under that level. For example, to view all groups that you created under root, enter / as the hierarchy level.

7. Click **Apply**.

The page displays the groups that match the filter criteria.

8. **(Optional)** Perform the following:

- To hide the column filters, click **Disable**.

This action does not clear the filter criteria that you have set.

- To clear the filter criteria, click **Clear**.

---

## Filtering resources

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the left navigation pane, perform one of the following:
  - Click **Groups**.
  - Click **Resources** and continue with Step 5.
3. On the Group Management page, select a group to assign a resource to an existing group.
4. Perform one of the following:
  - Click **New > Assign Resources**.
  - Click **Edit > Assign Resources**.
  - Click **View > Edit > Assign Resources**.
5. On the Resources page, click **Filter: Enable** and perform the following:
  - a. In the **Name** field, enter the resource name.
  - b. In the **Type** field, select the resource type.
6. Click **Apply**.
7. **(Optional)** To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

### Result

The table displays the resources that match the filter criteria.



## Removing assigned resources from a group

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Groups**.
3. Perform one of the following:
  - Select the resources, and click **Remove** if you have assigned resources to the group while creating the group.
  - Select a group, and click **Edit > Remove**.
  - Select a group, and click **View > Edit > Remove**.

The system removes the association of the resource with the group.

## Group Management field descriptions

| Name                    | Description                                 |
|-------------------------|---------------------------------------------|
| <b>Select check box</b> | The option to select a group.               |
| <b>Name</b>             | The name of the group.                      |
| <b>Type</b>             | The group type based on the resources.      |
| <b>Hierarchy</b>        | The position of the group in the hierarchy. |
| <b>Description</b>      | A brief description of the group.           |

| Button                        | Description                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------|
| <b>View</b>                   | Displays the View Group page with details of the selected group.                                   |
| <b>Edit</b>                   | Displays the Edit Group page where you change the information of the selected group.               |
| <b>New</b>                    | Displays the Create Group page where you can create a new group.                                   |
| <b>Duplicate</b>              | Displays the Duplicate Group page where you can duplicate a group to another selected group.       |
| <b>Delete</b>                 | Deletes the selected groups.                                                                       |
| <b>More Actions &gt; Move</b> | Displays the Move page where you can move a group to another group.                                |
| <b>More Actions &gt; Sync</b> | Displays the Resource sync page that you use to synchronize resources of a specific resource type. |
| <b>Advanced Search</b>        | Displays fields where you can specify the criteria for searching a group.                          |
| <b>Filter: Enable</b>         | Displays fields where you can set the filter criteria. This button is a toggle button.             |

*Table continues...*

| Button                 | Description                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This button is a toggle button. |
| <b>Filter: Clear</b>   | Clears the filter criteria.                                                                           |
| <b>Filter: Apply</b>   | Filters groups based on the criteria.                                                                 |
| <b>Select: All</b>     | Selects all groups in the table.                                                                      |
| <b>Select: None</b>    | Clears all check boxes.                                                                               |

| Icon                                                                              | Description                      |
|-----------------------------------------------------------------------------------|----------------------------------|
|  | Refreshes the group information. |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link in the top-right corner of the page.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>The criteria for search operation. The page displays the following fields:</p> <ul style="list-style-type: none"> <li>• <b>Field 1</b>: The list of criteria to search groups.</li> <li>• <b>Field 2</b>: The list of operators for evaluating the expression. This list of operators depends on the criterion that you selected in <b>Field 1</b>.</li> <li>• <b>Field 3</b>: The value of the search criterion. The Group Management service retrieves and displays the groups that match this value.</li> </ul> |

| Icon | Description                                                                                          |
|------|------------------------------------------------------------------------------------------------------|
| +    | Adds a row below <b>Field 1</b> , <b>Field 2</b> , and <b>Field 3</b> to add more search conditions. |
| -    | Deletes the row with the search conditions.                                                          |

| Button        | Description                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Clear</b>  | Clears the search value that you entered in <b>Field 3</b> .                                                       |
| <b>Search</b> | Searches the group based on the specified search conditions and displays the results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancel the search operation and hides the <b>Criteria</b> section.                                                 |

## New Group field descriptions

### New Group

| Field       | Description                   |
|-------------|-------------------------------|
| <b>Name</b> | The unique name of the group. |

*Table continues...*

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>             | <p>The group type based on the resources. The options are:</p> <ul style="list-style-type: none"> <li>• <b>&lt;Resource&gt;</b>: To create a group with members of the same resource type.</li> <li>• <b>All</b>: To create a group without any restrictions on the members of the group.</li> </ul> <p> <b>Note:</b><br/>You cannot change the group after you create a group.</p>                                                                                                                                                                                                                                                                                                                |
| <b>Group Membership</b> | <p>The group type based on the resources. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Query Based</b>: To create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only resource type query groups. Thus, these groups cannot have subgroups.</li> <li>• <b>Selection Based</b>: To create a group that contains resources based on static assignment. The groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types.</li> </ul> <p> <b>Note:</b><br/>You can create up to 400 members in a group.</p> |
| <b>Description</b>      | A brief description of the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Button                  | Description                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assign Resources</b> | <p>Displays the Resources page where you can search and assign resources to a group.</p> <p> <b>Note:</b><br/>The <b>Assign Resources</b> button is available only when you select <b>Selection Based</b> for creating group members in the group.</p> |
| <b>Commit</b>           | Creates a new group with the specified configurations.                                                                                                                                                                                                                                                                                    |
| <b>Cancel</b>           | Discards the changes that you made to the Create Group page and displays the Group management page.                                                                                                                                                                                                                                       |

## Define Query

The page displays the following fields when you select **Query Based** for creating group members:

| Field       | Description               |
|-------------|---------------------------|
| <b>Name</b> | The name of the resource. |
| <b>Type</b> | The resource type.        |

*Table continues...*

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Define Query</b>  | Displays the following fields: <ul style="list-style-type: none"> <li>• <b>Field 1:</b> The list of criteria that you can use to search resources.</li> <li>• <b>Field 2:</b> The list of operators for evaluating the expression. The list of operators depends on the criterion that you selected in <b>Field 1</b>.</li> <li>• <b>Field 3:</b> The value corresponding to the search criteria.</li> </ul> |
| Button               | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
| +                    | Adds a search condition row for defining the new search condition.                                                                                                                                                                                                                                                                                                                                           |
| –                    | Removes a search condition.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Execute Query</b> | Runs the query and fetches resources matching the search conditions defined in the query. The page displays the resources in the <b>Results</b> section.<br><br> <b>Note:</b><br>The system displays the <b>Execute Query</b> button only when you create a query-based group.                                              |

## Assigned Resources

The page displays the following fields when you select **Selection Based** for creating group members:

| Field                   | Description                                                                         |
|-------------------------|-------------------------------------------------------------------------------------|
| <b>Name</b>             | The name of the resource.                                                           |
| <b>Type</b>             | The resource type.                                                                  |
| Button                  | Description                                                                         |
| <b>Assign Resources</b> | Displays the Resources page that you use to search and assign resources to a group. |
| <b>Remove</b>           | Removes the selected resources from the list of assigned resources.                 |

## View Group field descriptions

### View Group

| Field       | Description                            |
|-------------|----------------------------------------|
| <b>Name</b> | The unique name of the group.          |
| <b>Type</b> | The resources that the group contains. |

*Table continues...*

| Field                   | Description                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group Membership</b> | The group type that is based on the resources. The options are: <ul style="list-style-type: none"> <li>• If the group is selection-based, the system displays the assigned resources.</li> <li>• If the group is query-based, click <b>Execute Query</b> to view the assigned resources.</li> </ul> |
| <b>Description</b>      | A brief description of the group.                                                                                                                                                                                                                                                                   |

| Button      | Description                                                            |
|-------------|------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Group page where you can edit the group information. |
| <b>Done</b> | Closes the View Group page and displays the Group Management page.     |

## Define Query

The page displays the following fields when you use the **Query Based** option for creating group members:

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Define Query</b> | Displays the following fields: <ul style="list-style-type: none"> <li>• <b>Field 1:</b> The list of criteria that you can use to search resources.</li> <li>• <b>Field 2:</b> The list of operators for evaluating the expression. The list of operators depends on the criterion that you selected in <b>Field 1</b>.</li> <li>• <b>Field 3:</b> The value corresponding to the search criteria.</li> </ul> |

| Button               | Description                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>+</b>             | Adds a search condition row for defining a new search condition.                                                                                                                                                                                                                                                                                                      |
| <b>–</b>             | Removes the search condition.                                                                                                                                                                                                                                                                                                                                         |
| <b>Execute Query</b> | Runs the query and fetches resources matching the search conditions defined in the query. The page displays the resources in the <b>Results</b> section. <p> <b>Note:</b></p> <p>The system displays the <b>Execute Query</b> button only when you create a query-based group.</p> |

The page displays the following fields for assigned resources:

| Field       | Description              |
|-------------|--------------------------|
| <b>Name</b> | The name of the resource |
| <b>Type</b> | The resource type        |

## Edit Group field descriptions

You can edit a group. However, you cannot edit the following fields:

- **Type**
- **Group Membership**

### Edit Group

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>             | The unique name of the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Type</b>             | The group type based on the resources. The options are: <ul style="list-style-type: none"> <li>• <b>&lt;Resource&gt;</b>: To create a group with members of the same resource type.</li> <li>• <b>All</b>: To create a group without any restrictions on the members of the group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Group Membership</b> | The group type based on the resources. The options are: <ul style="list-style-type: none"> <li>• <b>Query Based</b>: To create a group that contains resources that match a specific query criteria. Query-based groups can have resources only of a specific type. You can create only resource type query groups. Thus, these groups cannot have subgroups.</li> <li>• <b>Selection Based</b>: To create a group that contains resources based on static assignment. The groups can have subgroups. Subgroups and parent group might have members of the same resource type or different resource types.</li> </ul> <p> <b>Note:</b><br/>You cannot change the group after you create a group.</p> |
| <b>Description</b>      | A brief description of the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Button        | Description                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes in the database.                                                                |
| <b>Cancel</b> | Discards the changes that you made on the Edit Group page and displays the Group Management page. |

### Define Query

The page displays the following fields when you select **Query Based** for creating group members:

| Field       | Description               |
|-------------|---------------------------|
| <b>Name</b> | The name of the resource. |
| <b>Type</b> | The resource type.        |

*Table continues...*

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Define Query</b> | Displays the following fields: <ul style="list-style-type: none"> <li>• <b>Field 1:</b> The list of criteria that you can use to search resources.</li> <li>• <b>Field 2:</b> The list of operators for evaluating the expression. The list of operators depends on the criterion that you selected in <b>Field 1</b>.</li> <li>• <b>Field 3:</b> The value corresponding to the search criteria.</li> </ul> |

| Button               | Description                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| +                    | Adds a row for defining a new search condition.                                                                                                                                                                                                                                                                                                                 |
| –                    | Removes the row that defines the search condition.                                                                                                                                                                                                                                                                                                              |
| <b>Execute Query</b> | Runs the query and fetches resources matching the search conditions defined in the query. The page displays the resources in the <b>Results</b> section.<br><br> <b>Note:</b><br>The system displays the <b>Execute Query</b> button only when you create a query-based group. |

## Assigned Resources

The page displays the following fields when you select the **Selection Based** option for creating group members:

| Field       | Description              |
|-------------|--------------------------|
| <b>Name</b> | The name of the resource |
| <b>Type</b> | The type of the resource |

| Button                  | Description                                                                      |
|-------------------------|----------------------------------------------------------------------------------|
| <b>Assign Resources</b> | Displays the Resources page where you can search and assign resources to a group |
| <b>Remove</b>           | Removes the selected resources from the list of assigned resources               |

## Delete Group Confirmation field descriptions

| Field                 | Description                                 |
|-----------------------|---------------------------------------------|
| <b>Name</b>           | The name of the group                       |
| <b>Type</b>           | The group type based on the resources       |
| <b>Hierarchy</b>      | The position of the group in the hierarchy  |
| <b>Description</b>    | A brief description of the group            |
| <b>Subgroup Count</b> | The number of subgroups in the parent group |
| <b>Resource Count</b> | The number of resources in the group        |

| Button | Description                                                          |
|--------|----------------------------------------------------------------------|
| Delete | Deletes the groups listed in the table.                              |
| Cancel | Cancels the delete operation and displays the Group Management page. |

---

## Duplicate Group field descriptions

| Name        | Description                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select      | The option to select a group.                                                                                                                                                                                                                                                                                                |
| Name        | The groups under which you can create a copy of the selected group. Use the plus sign (+) to expand a group.                                                                                                                                                                                                                 |
| Type        | The group type based on resources.                                                                                                                                                                                                                                                                                           |
| Dynamic     | The status that indicates whether the group uses a query to determine the members or contains static members. The options are: <ul style="list-style-type: none"> <li>• <b>true</b>: Indicates that group membership is not permanent.</li> <li>• <b>false</b>: Indicates that the group contains static members.</li> </ul> |
| Description | A brief description of the group.                                                                                                                                                                                                                                                                                            |

| Button         | Description                                                     |
|----------------|-----------------------------------------------------------------|
| Root           | Creates a copy of the selected group at the root level.         |
| Selected Group | Creates a copy of the group that you selected within the group. |
| Cancel         | Discards the changes and displays the Group Management page.    |

---

## Move Group field descriptions

Use this page to move a group to another group or to root level.

| Name        | Description                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select      | The option to select a group.                                                                                                                                                                                                                                                                                                |
| Name        | The groups to which you can move the selected group. Use the plus sign (+) to expand a group.                                                                                                                                                                                                                                |
| Type        | The group type based on resources.                                                                                                                                                                                                                                                                                           |
| Dynamic     | The status that indicates whether the group uses a query to determine the members or contains static members. The options are: <ul style="list-style-type: none"> <li>• <b>true</b>: Indicates that group membership is not permanent.</li> <li>• <b>false</b>: Indicates that the group contains static members.</li> </ul> |
| Description | A brief description of the group.                                                                                                                                                                                                                                                                                            |



| Button                | Description                                                                        |
|-----------------------|------------------------------------------------------------------------------------|
| <b>Root</b>           | Moves the selected group to the root level.                                        |
| <b>Selected Group</b> | Moves the selected group to the group that you selected in the <b>Name</b> column. |
| <b>Cancel</b>         | Closes the Move Group page and returns to the Group Management page.               |

---

## Resource Synchronization field descriptions

| Name        | Description       |
|-------------|-------------------|
| <b>Type</b> | The resource type |

| Button        | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Sync</b>   | Synchronizes resources for the selected resource type and displays the Group Management page.                   |
| <b>Cancel</b> | Discards the changes that you made to the Resource Synchronization page and displays the Group Management page. |

---

## Managing resources

---

### Manage resources

System Manager contains different types of resources such as users and roles. You can view and filter these resources based on the search criteria. You can also add resources of the same or different types in a group.

---

## Accessing resources

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Resources**.

### Related links

[Resources field descriptions](#) on page 178

---

## Assigning resources to a new group

### About this task

Use this functionality to create a new group and assign resources to the group. You can choose to create the new group at root level or within an existing group.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Resources**.
3. On the Resources page, select a resource from the list or click **Advanced Search** to search for a resource.
4. Click **Add To New Group**.
5. To add a resource to a new group at root level, do the following:
  - a. On the Choose Parent Group page, click **Root**.
  - b. On the Create Group page, enter the appropriate information.
  - c. Click **Commit**.
6. To add a resource to a new subgroup within a group, do the following:
  - a. On the Choose Parent Group page, click a group.  
To select a subgroup of a group, click **+** and click the subgroup.
  - b. Click **Selected Group**.
  - c. On the Create Group page, enter the appropriate information.  
  
The system creates the new group and assigns the selected resources. The system adds the new group within the group that you selected on the Choose Parent Group page.
  - d. Click **Commit**.

### Related links

[Resources field descriptions](#) on page 178

[New Group field descriptions](#) on page 168

---

## Adding resources to a selected group

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Resources**.
3. Select a resource from the resource table.

You can also click the **Advanced Search** link to search a resource.

4. Click **Add To Group**.
5. On the Choose Group page, click a group.
6. Click **Selected Group**.

The Group Management module assigns the selected resources to the selected groups on the Choose Group page.

#### Related links

[Resources field descriptions](#) on page 178

---

## Searching for resources

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Resources**.
3. On the Resources page, click **Advanced Search**.
4. In the **Criteria** section, in the **Type** field, select a resource type.
5. In the **Resource Attributes** section, perform the following steps:
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter search value in the third field.
6. **(Optional)** To add another search condition, click the plus sign (+).

Click the minus sign (–) to delete a search condition. You can delete a search condition only if you have more than one search condition.

7. In the drop-down field, click **AND** or **OR**.

The system displays this option when you use the plus sign (+) to add a search condition.

8. Click **Search**.

The Resources section displays the resources matching the search criteria. If no resources match the search criteria, system displays the message `No records are found`.

---

## Filtering resources

### About this task

You can filter and view resources that meet the specified selection criteria. Applying the filters requires you to specify the filter criteria in the fields provided under columns in the table displaying the resources. The column titles are the filter criteria. You can filter resources on multiple filter criteria.

## Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Resources**.
3. On the Resources page, click **Filter: Enable**.
4. Type the resource name in the **ID** field.

You can apply filter on one column or multiple columns.

5. Select the resource type from the **Type** field.
6. Click **Apply**.

To hide the column filters, click **Disable**. This action does not clear the filter criteria that you have set in the column filters.

The table displays resources that match the filter criteria.

## Resources field descriptions

### Resources section

| Name                | Description                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------|
| <b>Select</b>       | Use this check box to select a record.                                                              |
| <b>ID</b>           | The unique name of the resource. Also known as native ID of the resource                            |
| <b>Type</b>         | The type based on the resources.                                                                    |
| <b>View Details</b> | The link displays the attributes and membership details of the selected resources on the same page. |

| Button                  | Description                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add to Group</b>     | Displays the Choose Group page. Use this page to choose a group in which you want to add the selected resource.                     |
| <b>Add to New Group</b> | Displays the Choose Parent Group page. Use this page to add the selected resources to a new group or to a chosen group.             |
| <b>Cancel</b>           | Closes the Resources page and take you to the Create Group page.                                                                    |
| <b>Advanced Search</b>  | Displays fields that you can use to specify the search criteria for searching a resource.                                           |
| <b>Filter: Enable</b>   | Displays fields under the columns <b>ID</b> and <b>Type</b> . You can use them to set the filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>  | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                                      |
| <b>Filter: Apply</b>    | Filters the resources based on the filter criteria.                                                                                 |

*Table continues...*

| Button                                                                            | Description                                               |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------|
| Select: All                                                                       | Select all the resources in the table.                    |
| Select: None                                                                      | Clears the selection for the resources that you selected. |
|  | Refreshes the resource information in the table.          |

### Attributes of Resource section

| Field | Description                                           |
|-------|-------------------------------------------------------|
| Name  | The name of the attribute.                            |
| Value | The value assigned to the attribute for the resource. |

### Resource is member of following groups section

| Field       | Description                                        |
|-------------|----------------------------------------------------|
| Name        | The unique name of the group.                      |
| Type        | The group type based on the resources it contains. |
| Hierarchy   | The position of the group in the hierarchy.        |
| Description | A brief description about the group.               |

### Criteria section

Click **Advanced Search** to view this section. The **Advanced Search** link is available at the upper-right corner of the page.

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                | The types based on the resources it contains.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Resource Attributes | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>Drop-down 1: The criteria for searching a resource. The options are attributes of resources for the attribute type selected in the <b>Type</b> drop-down list.</li> <li>Drop-down 2: The list of operators for evaluating the expression. The list of operators depends on the type of attribute selected in the Drop-down 1 list.</li> <li>Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Button          | Description                                                        |
|-----------------|--------------------------------------------------------------------|
| Clear           | Clears the search value that you entered in the third field.       |
| Search          | Searches the resources matching the search conditions.             |
| Close           | Closes the Criteria section.                                       |
| Advanced Search | Cancel the search operation and hides the <b>Criteria</b> section. |

## Choose Group field descriptions

Use this page to add resources to the selected groups.

| Name               | Description                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select</b>      | The option to select a group.                                                                                                                                                                                                                                                                                                |
| <b>Name</b>        | The name of the group.                                                                                                                                                                                                                                                                                                       |
| <b>Type</b>        | The group type based on the type of resources. The options are: <ul style="list-style-type: none"> <li>• Groups with members of the same resource type.</li> <li>• All: Groups having members of any resource types.</li> </ul>                                                                                              |
| <b>Dynamic</b>     | The status that indicates whether the group uses a query to determine the members or contains static members. The options are: <ul style="list-style-type: none"> <li>• <b>true</b>: Indicates that group membership is not permanent.</li> <li>• <b>false</b>: Indicates that the group contains static members.</li> </ul> |
| <b>Description</b> | A brief description of the group.                                                                                                                                                                                                                                                                                            |

| Button                | Description                                                     |
|-----------------------|-----------------------------------------------------------------|
| <b>Expand All</b>     | Displays the subgroups of groups in the list.                   |
| <b>Collapse All</b>   | Hides the subgroups of all expanded groups.                     |
| <b>Selected Group</b> | Adds the resource as a member of the group you selected.        |
| <b>Cancel</b>         | Closes the Choose Group page and returns to the Resources page. |

## Choose Parent Group field descriptions

| Name               | Description                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select</b>      | Use this option to select a group.                                                                                                                                                                                                                                                          |
| <b>Name</b>        | The name of the group.                                                                                                                                                                                                                                                                      |
| <b>Type</b>        | The group type based on the type of resources. The options are: <ul style="list-style-type: none"> <li>• Groups with members of the same resource type.</li> <li>• All: Groups with members of any resource types.</li> </ul>                                                               |
| <b>Dynamic</b>     | Indicates whether the group uses a query to determine its members or has static members. The options are: <ul style="list-style-type: none"> <li>• <b>True</b>: Indicates that group membership is not permanent.</li> <li>• <b>False</b>: Indicates groups with static members.</li> </ul> |
| <b>Description</b> | A brief description of the group.                                                                                                                                                                                                                                                           |

| Button                                                                            | Description                                                                                                          |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Expand All</b>                                                                 | Displays the subgroups of groups listed in the table.                                                                |
| <b>Collapse All</b>                                                               | Hides the subgroups of all the expanded groups.                                                                      |
| <b>Root</b>                                                                       | Displays the New Group page. Use this page to create a new group. The selected resource is the member of this group. |
| <b>Selected Group</b>                                                             | Adds the resource as a member of the selected group.                                                                 |
|  | Refreshes the resource information in the table.                                                                     |
| <b>Cancel</b>                                                                     | Closes the Choose Parent Group page and displays the Resources page.                                                 |

---

## Managing roles

---

### Role Based Access Control

In System Manager, you require appropriate permissions to perform a task. The administrator grants permissions to users by assigning appropriate roles. Role Based Access Control (RBAC) in System Manager supports the following types of roles:

- Built-in
- Custom

With these roles, you can gain access to various elements with specific permission mappings.

Built-in roles are default roles that authorize users to perform common administrative tasks. You can assign built-in roles to users, but you cannot delete roles or change permission mappings in the built-in roles.

You can perform LDAP synchronization of Microsoft Active Directory or other supported directory server administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

 **Note:**

Granular RBAC is not supported for managing Avaya Meetings Server, Web Gateway, and Work Assignment elements by creating custom roles.

#### Related links

[Custom roles](#) on page 186

[Built-in roles](#) on page 182

## Built-in roles

| Role                                   | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auditor                                | Gives read-only access to logs, configuration information, and audit files. With this role, you cannot run any command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| System Administrator                   | <p>Gives the super-user privilege.</p> <p>System Administrator is the single all powerful role. With this role, you can perform operations, such as the following:</p> <ul style="list-style-type: none"> <li>• Backup and restore</li> <li>• Scheduling jobs</li> <li>• Bulk import and export</li> <li>• Tenant administration</li> <li>• Geographic Redundancy operations</li> <li>• Element and user management</li> <li>• Software upgrade</li> </ul> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• The System Administrator role replaces the Network Administrator role. System Manager does not support the Network Administrator role.</li> <li>• The page might not display all privileges that the System Administrator role supports. However, the system maps the permissions by implicit wild card rules.</li> </ul> |
| Avaya Services Administrator           | <p>This role is equivalent to the System Administrator role.</p> <p>Depending on the access level that is set in the <b>E-token Authentication</b> section on the External Authentication page, System Manager assigns this role to the service personnel who logs in to the system through Etoken.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Avaya Services Maintenance and Support | <p>Gives read-only access to maintenance logs, the capability to run diagnostics, and view the output of diagnostics tools. Using this role, you cannot run any command that might provide access to another host.</p> <p>System Manager assigns the role to the service personnel who logs in to the system through Etoken. The access level for the role depends on the value that is set in the <b>E-token Authentication</b> section on the External Authentication page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Backup Administrator                   | Gives access to create backups, schedule backups, and restore backups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

*Table continues...*



| Role                                    | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Provider Administrator template | <p>Gives permissions to:</p> <ul style="list-style-type: none"> <li>• Configure the solution</li> <li>• Manage the organization hierarchy of tenants. For example, site, department, and team.</li> <li>• Assign elements and resource permissions to the site</li> <li>• Manage end users for the tenant</li> <li>• Manage Tenant Administrators and Site Administrators</li> </ul> <p> <b>Note:</b><br/>Service Provider Administrator Template is a template role.</p> |
| Tenant Administrator Template           | <p>Gives permissions to:</p> <ul style="list-style-type: none"> <li>• Manage end users for the tenant</li> <li>• Communication Manager webpages</li> </ul> <p> <b>Note:</b><br/>Tenant Administrator Template is a template role.</p>                                                                                                                                                                                                                                     |
| Discovery Admin                         | Gives permissions to configure the discovery parameters such as SNMP version, SNMP credentials, the subnetworks, and devices that you require to discover. You also have the permissions to schedule and run a discovery operation.                                                                                                                                                                                                                                                                                                                        |
| End-User                                | <p>The administrator assigns this role to the telephony users.</p> <p> <b>Important:</b><br/>You cannot log in to System Manager with the End-User role.</p>                                                                                                                                                                                                                                                                                                            |
| Avaya Breeze Admin                      | Gives read-write access to the Avaya Breeze® platform configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Avaya Breeze Auditor                    | Gives read-only access to Avaya Breeze® platform logs, configuration information, and audit files. With the Auditor role, you cannot run any command that might provide access to another host.                                                                                                                                                                                                                                                                                                                                                            |
| Avaya Breeze Server Admin               | Gives read and write access to all Avaya Breeze® platform management functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Avaya Breeze Service Profile Admin      | Gives write access only for Service Profiles.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Avaya Breeze Services Admin             | Gives write access only for Service Management.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Communication Manager Admin             | Gives you access and permission to perform all activities related to Communication Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Messaging System Admin                  | Gives you access and permission to perform all activities related to Messaging or mailbox. You cannot perform any tasks related to Communication Manager as a Modular Messaging administrator.                                                                                                                                                                                                                                                                                                                                                             |
| Presence Admin                          | Gives read-write access to the Presence configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table continues...

| Role                          | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Presence Auditor              | Gives read-only access to logs, configuration information, and audit files. With the Auditor role you cannot run any command that might provide access to another host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Security Administrator        | Gives read-write access to create other logins, create, modify or assign roles, install ASG keys, install licenses, and install PKI certificates and keys.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SIP AS Auditor                | Gives read-only access to all SIP Foundation server management functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SIP AS Security Administrator | Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SIP AS System Administrator   | Gives read and write access to all SIP Foundation server management functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| CS1000_Admin1                 | <p>Gives unrestricted OAM access to most administrative functions and provisioning for all customers on all call servers and related elements. However, the role does not give access to the security and account administration. The role includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, update, and SNMP management for CS 1000 systems. Gives authorization to use all roles on all User Management elements with all permissions.</p> <p>You can access the following elements:</p> <ul style="list-style-type: none"> <li>• All elements of type: CS 1000</li> <li>• All elements of type: Deployment Manager</li> <li>• All elements of type: Linux Base</li> <li>• All elements of type: Patching Manager</li> <li>• All elements of type: SNMP Manager</li> </ul> <p>As this role gives permissions to All elements of type: Linux Base, you cannot use this role if you only require authorization to manage CS 1000 systems. The administrator must create a custom role for the user who requires to manage CS 1000 systems.</p> |

*Table continues...*

| Role                 | Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CS1000_Admin2        | <p>Provides unrestricted OAM access including security and account administration, and provisioning for all customers on all call server elements. The role also includes basic diagnostic (PDT1) privileges and access to network-level services for deployment, patching, SNMP, IPsec and SFTP management for CS 1000 systems.</p> <p>You can access the following elements:</p> <ul style="list-style-type: none"> <li>• All elements of type: CS1000</li> <li>• All elements of type: Deployment Manager</li> <li>• All elements of type: IPSec Manager</li> <li>• All elements of type: Linux Base</li> <li>• All elements of type: Patching Manager</li> <li>• All elements of type: Secure FTP Token Manager</li> <li>• All elements of type: SNMP Manager</li> </ul> <p>As this role gives permissions to All elements of type: Linux Base, you cannot use this role if you only require authorization to manage CS 1000 systems. The administrator must create a custom role for the user who requires to manage CS 1000 systems.</p> |
| CS1000_CLI_Registrar | <p>Provides permission to register and unregister each CS 1000 elements, such as Call Server, MGC, and Media Card, using the local device OAM CLI. The role has a single permission value to allow or deny a user to register or unregister an element.</p> <p>You can access the following elements:</p> <ul style="list-style-type: none"> <li>• All elements of type: CS1000</li> <li>• All elements of type: Linux Base</li> </ul> <p>The role does not have CS 1000 security or network level security privileges. The installation and repair technicians specifically require this role.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| CS1000_PDT2          | <p>Gives full diagnostic and operating system access to all call servers. The role restricts access to administrative functions and customer provisioning data unless combined with another role.</p> <p>You can access All elements of type: CS1000.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MemberRegistrar      | <p>Gives limited access. You can register new members to the primary server.</p> <p>You can access the following elements:</p> <ul style="list-style-type: none"> <li>• All elements of type: IPSec Manager</li> <li>• All elements of type: LinuxBase</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

*Table continues...*

| Role               | Privileges                                                                                                                                                                                                                                                           |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Patcher            | <p>Gives access to software maintenance functions, such as update and maintenance. You can access the following elements:</p> <ul style="list-style-type: none"> <li>• All elements of type: Linux Base</li> <li>• All elements of type: Patching Manager</li> </ul> |
| Service Technician | <p>The system assigns the role to the service personnel when the service personnel connects to customer systems through the e-token. The Service Technician role has limited privileges as compared to the Avaya Services Administrator role.</p>                    |

## Custom roles

On the Roles page, you can create a custom role that maps to specific elements of different types and specify customized permissions for the elements.

You can assign the roles that you created to users to perform specific tasks on an element. For example, a custom role that you create for a single element can only perform specific tasks on that element. A permission set defines the tasks that you can perform on the element with this role.

You can also define roles that apply to how elements and element types are hierarchically arranged in user-defined groups. When you map a permission to a group, the system takes that group into account when determining user permissions.

### Note:

- When a user who is associated with custom role administers various operations on Communication Manager, which is managed by System Manager, then custom role requires permissions for Scheduler and Communication Manager templates along with required Communication Manager admin permissions. Therefore, custom role must have minimum permissions:
  - For on demand job create/view permissions in Scheduler.
  - To view Communication Manager templates.
- If Communication Manager IP address is changed on the **Inventory > Manage Elements** page, custom users that have roles for that particular Communication Manager cannot access those Communication Managers.

For example, the Communication Manager IP Address can be changed on the Manage Elements page for the following reasons:

- Duplex Communication Manager gets interchanged
- Communication Manager IP Address has been updated manually

If Communication Manager IP Address is changed on the Manage Elements page, you must also update the corresponding Communication Manager role mappings.

## Viewing user roles

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role.

In the right pane, the system displays the role name, a description, and the number of users, and also the elements that you can access by using the role.

### Related links

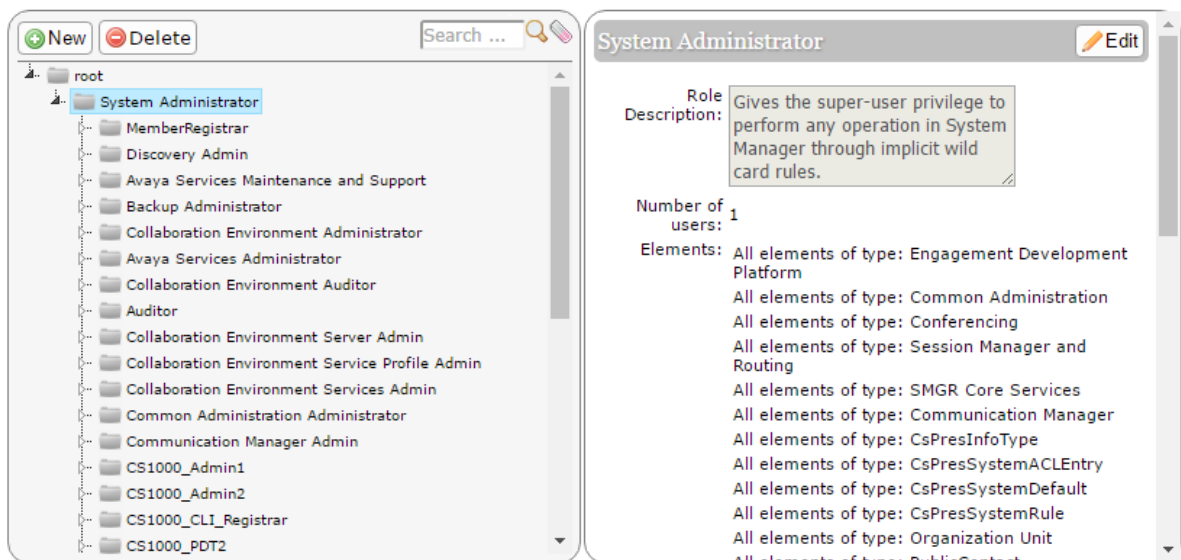
[Roles field descriptions](#) on page 194

## Adding a custom role

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role, and perform one of the following:
  - Click **New**.
  - Right-click and select **New**.

The role that you select becomes the parent of the role that you create. The permissions available to the new role are limited to the permissions of the parent role.



On the Add New Role page, the system displays the parent role in the **Parent Role Name** field.

4. Type the relevant information in **Role Name** and **Role Description** fields.

5. Click **Commit and Continue**.

The system displays the Role Details page.

6. On the **Element/Service Permissions** tab, click **Add mapping** to define permissions for a role.

You can also click **Copy All From** to copy all the permissions on all types of elements or services from an existing role. For instructions, see Copying permission mapping for a role.

7. Select a group from the **Group Name** field.

Ensure that you create a group before you select the group. For instructions, see Creating groups. For instructions to assign resources to a group, see Assigning resources to a group.

8. **(Optional)** If you leave the **Group Name** field blank, in the **Element or Resource Type** field, click an element or **All**.

9. Click **Next**.

The title of the Permission Mapping page displays the element type that you selected.

10. On the Permission Mapping page, change the permissions that are available for this role as appropriate.

The system displays the permissions that are available for the parent of the role that you created. The system also displays unassigned permissions in a read-only format. Only an administrator can deny, change, or view the permissions for the role.

11. Click **Commit**.

The system displays the Role Details page and the selected permissions.

12. Click **Commit**.

## Related links

[Copying permission mapping for a role](#) on page 193

[Creating groups](#) on page 160

[Assigning resources to a group](#) on page 163

[Add Mapping field descriptions](#) on page 196

[Add New Role field descriptions](#) on page 195

[Mapping permissions by using the template](#) on page 191

## Adding a custom tenant administrator role

### Procedure

1. On the System Manager web console, click **Services > Tenant Management** and perform the following:
  - a. Create a tenant.
  - b. Add the level 1 organization hierarchy or site to the tenant.
  - c. **(Optional)** Add the level 2 and level 3 organization hierarchy to the tenant.  
For more information, see [Creating a tenant](#).
2. On the System Manager web console, click **Users > Groups & Roles**.
3. In the navigation pane, click **Roles**.
4. On the Roles page, select **System Administrator** and perform one of the following:
  - Click **New**.
  - Right-click and select **New**.
5. On the Add New Role page, enter the values in the **Role Name** and **Role Description** fields.
6. Click **Commit and Continue**.  
The system displays the Role Details page.
7. Click **Copy All From**.
8. In the **Copy from Role** field, click **Tenant Administrator Template**.
9. Click **Copy**.
10. On the Role Details page, click **Add Mapping**.
11. On the Select Element and/or Network Service to Map to Role page, perform the following:
  - a. In **Element or Resource Type**, click **Organization Unit**.
  - b. In **Element or Resource Instance**, click the name of the tenant that you created in Step 1, and click **Next**.
  - c. Select **All** or **Create, Delete, Edit**, or **View** to set the appropriate permissions.
  - d. Click **Commit**.
12. Perform Step 8 and Step 9 to provide appropriate permissions to the tenant for the following organization hierarchy:
  - Level 1 or the site
  - (Optional) Level 2 or the department
  - (Optional) Level 3 or the team

In the **Element or Resource Instance** field, click site, department, or team as appropriate to which you want to set permissions. See Step 11b.

13. **(Optional)** On the Role Details page, click **Add Mapping**, and provide permission mapping.
14. Click **Commit** to confirm your settings.

#### Related links

[Creating a tenant](#) on page 1256

---

## Assigning permissions to access Solution Deployment Manager

### About this task

System Manager provides access permissions to Solution Deployment Manager through Role Based Access Control (RBAC) for elements, such as Communication Manager, Session Manager, Branch Session Manager, and IP Office. System Manager defines flexible access privileges for deployment, migration, upgrade, and update so that the users with administrator credentials can create their own roles.

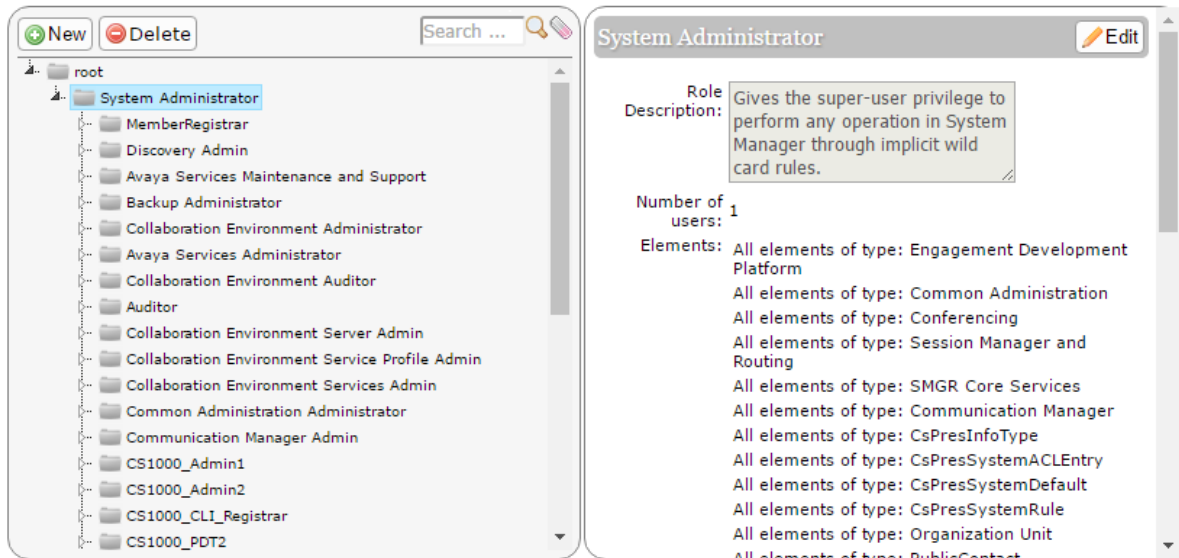
With RBAC, System Manager supports access privileges at the element level and physical location level.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
  - Click **New**.
  - Right-click and select **New**.

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.





4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, select **Solution Deployment Manager**.
9. In the **Element or Resource Instance** field, select **All**.
10. Click **Next**.
11. In Upgrade Management and VM Management, select appropriate permissions, and click **Commit**.

The user can now access the Solution Deployment Manager links.

To assign user permissions, select **Users** in **Element or Resource Type**. Select appropriate permissions, and click **Commit**.

## Mapping permissions by using the template

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. In the **Element/Service Permissions** tab, click **Add Mapping**.
5. In the **Element or Resource Type** field, select an element, for example, CS 1000.

6. Click **Next**.

The system displays the permission mapping for the element that you selected.

7. Perform the following as appropriate to modify permissions:

- a. Select a different permission from the **Template for permission set** field.
- b. Select permissions.
- c. Clear permissions.

8. Click **Commit**.

### Related links

[Permission mapping field descriptions](#) on page 197

---

## Assigning users to a role

To assign a role to an end user, follow the instructions outlined in Assigning roles to a user. An end user is a user with no role or the End-User role.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Assigned Users** tab.
5. Click **Select Users** to assign a role to users or edit a role.

The system displays the Assigned Users page.

 **Note:**

The system does not display end users in the **Assigned Users** list. You can assign a role to an end user from **User Management > Manage Users**. For more information, see Assigning roles to a user.

6. Select users to whom you want to assign the role.
7. Click **Commit**.

The system displays the permissions for the role on the Role Details page.

### Related links

[Assigning roles to a user](#) on page 249

[Assigned Users field descriptions](#) on page 197

---

## Unassigning users from role

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Assigned Users** tab.
5. Click **Selected Users**.
6. On the Assigned Users page, clear the check box of the user whom you want to unassign.
7. Click **Commit**.

---

## Copying permission mapping for a role

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Element/Service Permissions** tab.
5. Click **Copy All From**.

The system displays the Permission Mapping page.

6. In the **Copy From Role** field, select a role.

The system displays all child roles of the parent of this role and all child roles of this role.

 **Note:**

Using the **Copy From Role** option, you cannot copy permissions from the System Administrator role.

7. Click **Copy**.

The system displays the Role Details page

8. Click **Commit**.

The system displays the Roles page where you can view the details of the role.

### Related links

[Permission mapping field descriptions](#) on page 197

---

## Editing a custom role

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, edit the **Role Name** and **Description** fields.
5. Click **Commit and Continue**.
6. On the **Element/Service Permissions** tab, click **Add mapping** and change the permissions for a role as appropriate.  
For more information, see Mapping permissions using the template.
7. Click **Commit**.

### Related links

[Mapping permissions by using the template](#) on page 191

---

## Deleting custom roles

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select one or more roles that you must delete and perform one of the following:
  - Click **Delete**.
  - Right-click and select **Delete**.
4. On the Delete Roles page, click **Delete** to continue with the deletion.

When you delete a role, the system deletes all child roles of the role.

You cannot delete the implicit roles from the Roles page. However, the system deletes the implicit roles when the administrator deletes the tenant or site.

---

## Roles field descriptions

The Roles page contains two panes. The left pane displays the tree structure of roles. The right pane displays the details of the role that you select on the left pane.

| Name                    | Description                                      |
|-------------------------|--------------------------------------------------|
| <b>Role Description</b> | A brief description of the role                  |
| <b>No of users</b>      | The number of users associated with the role     |
| <b>Elements</b>         | The name of elements that are mapped to the role |

| Button        | Description                                                                           |
|---------------|---------------------------------------------------------------------------------------|
| <b>New</b>    | Displays the Add New Role page where you can add a custom role.                       |
| <b>Delete</b> | Displays the Delete Roles page where you can confirm the deletion of the custom role. |
| <b>Edit</b>   | Displays the Role Details page where you can change the custom role.                  |

| Icon                                                                              | Description                                     |
|-----------------------------------------------------------------------------------|-------------------------------------------------|
|  | Searches for the role based on the search text. |
|  | Clears the search text.                         |

## Add New Role field descriptions

| Name                    | Description                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parent Role Name</b> | The parent role that you selected on the Roles page to create the new role.<br><b>Parent Role Name</b> is a read-only field.                                                                |
| <b>Role Name</b>        | The name of the custom role that you want to add.<br>The name must be 1 to 256 characters long and can include characters: a-z, A-Z, 0-9, -, _, and space.<br>You can add up to 1500 roles. |
| <b>Role Description</b> | A brief description of the role.                                                                                                                                                            |

| Button                     | Description                                                                  |
|----------------------------|------------------------------------------------------------------------------|
| <b>Commit and Continue</b> | Saves the role name and description and takes you to the Roles Details page. |
| <b>Cancel</b>              | Cancels the permission mapping and returns to the Roles page.                |

### Related links

[Copying permission mapping for a role](#) on page 193

[Creating groups](#) on page 160

[Assigning resources to a group](#) on page 163

## Role Details field descriptions

| Name                    | Description                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parent Role Name</b> | The parent role that you selected on the Roles page to create the new role.<br><b>Parent Role Name</b> is a read-only field.                               |
| <b>Role Name</b>        | The name of the custom role that you want to add.<br>The name must be 1 to 256 characters long and can include characters: a-z, A-Z, 0-9, -, _, and space. |
| <b>Description</b>      | A brief description of the role that you add.                                                                                                              |

| Button                | Description                                                                   |
|-----------------------|-------------------------------------------------------------------------------|
| <b>Commit</b>         | Saves the changes and returns to the Roles page.                              |
| <b>Cancel</b>         | Discards the changes to the permission mapping and returns to the Roles page. |
| <b>Add Mapping</b>    | Displays the permissions page where you can map permissions for the role.     |
| <b>Delete Mapping</b> | Displays the Delete Mapping page where you can delete a permissions set.      |
| <b>Copy All From</b>  | Displays the Permission Mapping page where you can copy a permission set.     |

## Add Mapping field descriptions

| Name                                | Description                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group Name</b>                   | The name of the group that you can select for the role. The options are: <ul style="list-style-type: none"> <li>When you select a group, the system disables the <b>Element or Resource Type</b> field.</li> <li>When you do not select a group, the <b>Element or Resource Type</b> field is mandatory.</li> </ul> |
| <b>Element or Resource Type</b>     | The element types that are available.<br>The system displays elements in <b>Element or Resource Instance</b> based on the element type that you select in this field.                                                                                                                                               |
| <b>Element or Resource Instance</b> | The elements that are available or the resource instance.<br>The field lists the available elements based on the element type that you selected in the <b>Element or Resource Type</b> field.<br>When you select a group in <b>Group Name</b> , the system disables the <b>Element or Resource Type</b> field.      |

| Button        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| <b>Next</b>   | Saves your changes in this page and takes you to the Permission Mapping page. |
| <b>Cancel</b> | Cancels your selection and takes you to the Roles Details page.               |

#### Related links

[Copying permission mapping for a role](#) on page 193

[Creating groups](#) on page 160

[Assigning resources to a group](#) on page 163

## Assigned Users field descriptions

The system displays the Assigned Users page when you click **Select Users** on the **Assigned Users** tab of the Role Details page. You can select users to grant permissions that are associated with this role.

| Name             | Description                                                                                                                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Name</b> | The name of the user that you assign to the role.                                                                                                                                                                                                                                    |
| <b>Full Name</b> | The full name of the user that is assigned to the role.                                                                                                                                                                                                                              |
| <b>Type</b>      | The type of user. The options are: <ul style="list-style-type: none"> <li>• <b>local</b>: Indicates that users are stored in the directory server of System Manager.</li> <li>• <b>external</b>: Indicates that users are stored in the directory server of the customer.</li> </ul> |

| Button        | Description                                              |
|---------------|----------------------------------------------------------|
| <b>Commit</b> | Assigns the selected users to the role.                  |
| <b>Cancel</b> | Cancels the action and returns to the Role Details page. |

## Permission mapping field descriptions

The page displays the following fields when you click **Add Mapping** on the Role Details page.

| Name                               | Description                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Template for permission set</b> | The permission to which you want to map the role.                                                   |
| <b>Select/Unselect All</b>         | A toggle button to select or clear the functions that users with a role can perform on the element. |

| Button        | Description                              |
|---------------|------------------------------------------|
| <b>Commit</b> | Maps the permissions to the custom role. |

*Table continues...*

| Button        | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| <b>Cancel</b> | Cancels the permission mapping action and returns to the Role Details page. |

The page displays the following fields when you click **Copy All From** on the Role Details page.

| Name                  | Description                                                                         |
|-----------------------|-------------------------------------------------------------------------------------|
| <b>Copy from Role</b> | The role from where you can copy all permission mappings for the element or service |

| Button        | Description                                                   |
|---------------|---------------------------------------------------------------|
| <b>Copy</b>   | Copies the permission mapping for your custom role.           |
| <b>Cancel</b> | Cancels the copy action and returns to the Role Details page. |



# Chapter 6: Granular role based access control

---

## Granular RBAC

With Granular role based access control (RBAC), you can restrict access to resources such as Communication Manager servers, and objects of the resources such as endpoints and hunt groups.

When you create a role, you must select the resources for which a user should have access. You can assign permissions, or a combination of permissions to users. The permissions include adding, editing, deleting, or duplicating objects.

For certain objects, you can provide restricted access for a specific range to achieve range-level granularity of permissions. For example, for endpoints, you can provide access to a particular range of extensions.

Using Granular RBAC, you can define the range for the following Communication Manager objects:

| Name                    | Supported range                                            |
|-------------------------|------------------------------------------------------------|
| Endpoint                | Endpoint extension ranges                                  |
| Agent                   | Agent extension ranges                                     |
| Announcement            | Announcement extension ranges                              |
| Audio Group             | 1–50                                                       |
| Best Service Routing    | 1–511                                                      |
| Holiday Table           | 1–999                                                      |
| Variables               | From A-Z and AA-ZZ for all Communication Manager templates |
| Vector                  | 1–8000                                                     |
| Vector Directory Number | Digits                                                     |
| Vector Routing Table    | 1–999                                                      |
| Service Hours Table     | 1–999                                                      |
| Coverage Answer Group   | 1–1500                                                     |
| Coverage Path           | 1–9999                                                     |
| Coverage Remote         | 1–10000                                                    |

*Table continues...*

| Name                        | Supported range                |
|-----------------------------|--------------------------------|
| Coverage Time of Day        | 1–1000                         |
| Off PBX Endpoint Mapping    | Off PBX Endpoint Mapping range |
| Group Page                  | 1–999                          |
| Hunt Group                  | 1–8000                         |
| Intercom Group              | 1–1024                         |
| Pickup Group                | 1–5000                         |
| Terminating Extension Group | 1–32                           |
| Route Pattern               | 1–2000                         |
| Class of Restriction        | 0–995                          |
| Uniform Dial Plan           | UDP range                      |

- The roles and permissions also apply to the classic view apart from the Communication Manager objects mentioned.
- Granular RBAC is not applicable when you view the Communication Manager objects by clicking **Element Cut Through**. However, to access **Element Cut Through**, you must have the Element Cut Through permissions.
- When you assign a role to a user, the range permissions are considered along with the operation permissions.
- You must log off and log in for any permission you assign to take effect.

## Implicit permissions required for Communication Manager objects

As a user, you require additional permissions to perform certain actions. The following table specifies the implicit permissions required for performing these actions:

| Steps | Action                                  | Implicit permissions that are required |
|-------|-----------------------------------------|----------------------------------------|
|       | Duplicating an endpoint                 | Add endpoint permission                |
|       | Adding endpoints in bulk                | Add endpoint permission                |
|       | Editing an endpoint extension           | Edit endpoint permission               |
|       | Changing global parameters of endpoints | Edit endpoint permission               |
|       | Swapping endpoints                      | Edit endpoint permission               |
|       | Deleting endpoints in bulk              | Delete endpoint permission             |

*Table continues...*

| Steps                                                                                                                                         | Action                                                                        | Implicit permissions that are required                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Edit a user with the help of the Agent communication profile.</li> <li>Import users in bulk</li> </ul> | Changing an extension with an existing extension                              | Edit permission and delete permission                                                                                                                      |
| <ul style="list-style-type: none"> <li>Edit a user using the Agent communication profile.</li> <li>Import users in bulk</li> </ul>            | Changing an extension with a new extension                                    | Add permission and delete permission                                                                                                                       |
| <ul style="list-style-type: none"> <li>Edit a user using the Agent communication profile.</li> <li>Import users in bulk</li> </ul>            | Changing other fields other than extension                                    | Edit permissions                                                                                                                                           |
| Check the port extension remove option, and assign an endpoint extension to an agent.                                                         | Deleting an endpoint                                                          | Delete agents and add agents permissions                                                                                                                   |
|                                                                                                                                               | Editing agents in bulk                                                        | Edit agents permission                                                                                                                                     |
|                                                                                                                                               | Adding agents in bulk                                                         | Add agents permission                                                                                                                                      |
|                                                                                                                                               | Deleting agents in bulk                                                       | Delete agents permission                                                                                                                                   |
|                                                                                                                                               | Adding or editing a Communication Manager instance through inventory          | One of the following permissions: <ul style="list-style-type: none"> <li>ALL</li> <li>Audit</li> <li>View Audit Report</li> <li>Synchronization</li> </ul> |
|                                                                                                                                               | Using File Transfer Settings in Announcements                                 | ALL in Announcements<br>Edit permission<br>Move permission                                                                                                 |
|                                                                                                                                               | Downloading backed up announcements<br>Setting compact flash in announcements | ALL in Announcements                                                                                                                                       |
|                                                                                                                                               | Downloading audio groups                                                      | ALL in Audio Group                                                                                                                                         |
|                                                                                                                                               | Adding entries for AAR and ARS analysis                                       | Add permission<br>Edit permission                                                                                                                          |
|                                                                                                                                               | Updating UDP entries                                                          | New permission<br>Edit permission                                                                                                                          |
|                                                                                                                                               | Manage UDP Group permission for a specific Communication Manager              | Manage UDP Group permission in Communication Manager                                                                                                       |

*Table continues...*

| Steps | Action                                                                          | Implicit permissions that are required               |
|-------|---------------------------------------------------------------------------------|------------------------------------------------------|
|       | Adding, viewing, editing, and removing UDP Groups across Communication Managers | Add permission<br>Edit permission<br>View permission |

---

## Sample scenario for the range feature

When you assign a range for Hunt Group, and go to the **Hunt Group > Switch to Classic View > New** page, the system prompts you to enter a qualifier. You can enter the hunt group number, or type `Next`, and click **Add** to add the next available group number.

- If you enter a group number that is not a part of the assigned range, the system displays an error message.
- If you enter a group number within the assigned range, the system displays the NCM screen, where you can complete the add operation.
- If you enter a group number that is already present, the system displays the `Identifier previously assigned` message.

---

## Assigning permissions in User Management

The range feature in endpoints and agents is also applicable in **User Management**. When you assign a range for endpoints and agents, as per the permissions that are defined, you can add, edit, delete, and duplicate only the extensions that are associated with the user. Range is validated when you assign an endpoint extension or an agent extension through the endpoint or agent editor.

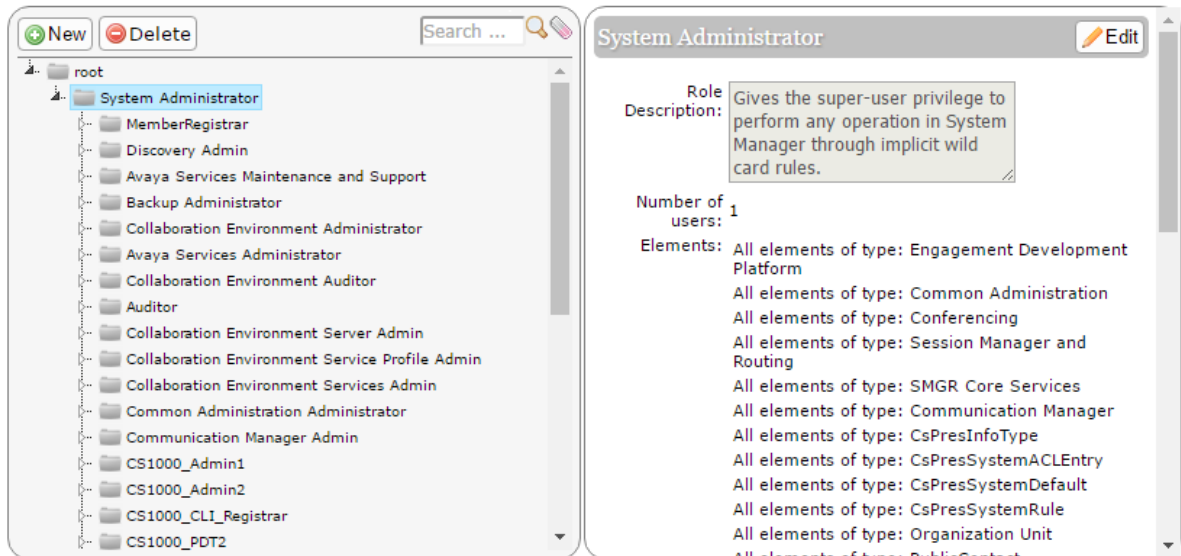
---

## Assigning permissions through User Management

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following:
  - Click **New**
  - Right-click and select **New**.

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, click **users**.
9. In the **Element or Resource Instance** field, click **All**.
10. Click **Next**.
11. On the Permission Mapping page, select the **Role Resource Type Action** and **Role Resource Type Attributes**. Enable **Administrative Users**, if required.
12. Click **Commit**.  
The system displays the Role Details page with the permission mapping you created.
13. Click **Add Mapping**.
14. To specify the operation resource type mapping, in the **Element or Resource Type** field, click **operation**.
15. Click **Next** and **Commit**.

---

## Field-level RBAC

System Manager supports field-level RBAC for Communication Manager objects. You can assign permissions for the following Communication Manager objects:

| Communication Manager object | Field                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Endpoints                    | <ul style="list-style-type: none"> <li>• Name</li> <li>• Security Code</li> <li>• IP Softphone</li> <li>• IP Video Softphone</li> <li>• EC500 State</li> <li>• EC500 Button</li> <li>• Coverage Path 1</li> <li>• Coverage Path 2</li> <li>• Tenant Number</li> <li>• Extension Number</li> <li>• Type</li> <li>• Port</li> <li>• Name</li> <li>• Lock Messages</li> <li>• Hunt-to Station</li> <li>• BCC</li> <li>• TN</li> <li>• Location</li> <li>• Loss Group</li> <li>• Speakerphone</li> <li>• Display Language</li> <li>• Survivable GK Node</li> <li>• Survivable COR</li> <li>• Survivable Trunk Dest</li> <li>• Message Lamp Ext</li> <li>• Mute Button Enabled</li> <li>• Media Complex Ext</li> <li>• Short/Prefixed Registration Allowed</li> <li>• LWC Reception</li> <li>• LWC Activation</li> <li>• LWC Log External Calls</li> <li>• CDR Privacy</li> </ul> |

*Table continues...*

| Communication Manager object | Field                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <ul style="list-style-type: none"> <li>• Redirect Notification</li> <li>• Per Button Ring Control</li> <li>• Bridged Call Alerting</li> <li>• Active Station Ringing</li> <li>• H.320 Conversion</li> <li>• 4Service Link Mode</li> <li>• Multimedia Mode</li> <li>• MWI Served User Type</li> <li>• AUDIX Name</li> <li>• IP Hoteling</li> <li>• Auto Select Any Idle Appearance</li> <li>• Coverage Msg Retrieval</li> <li>• Auto Answer</li> <li>• Data Restriction</li> <li>• Idle Appearance Preference</li> <li>• Bridged Idle Line Preference</li> <li>• EMU Login Allowed</li> <li>• Per Station CPN Send Calling No</li> <li>• Audile Message Waiting</li> <li>• Display Client Redirection</li> <li>• Select Last Used Appearance</li> <li>• Coverage After Forwarding</li> <li>• Multimedia Early Answer</li> <li>• Direct IP-IP Audio Connections</li> <li>• Always Use</li> <li>• IP Audio Hairpinning</li> <li>• Remote Softphone Emergency Calls</li> <li>• Emergency Location Ext</li> <li>• Conf/Trans on Primary Appearance</li> <li>• Bridged Appearance Origination Restriction</li> <li>• Call Appearance Display Format</li> <li>• IP Phone Group ID</li> </ul> |

*Table continues...*



| Communication Manager object | Field                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <ul style="list-style-type: none"> <li>• Hot Line Destination – Abbreviated Dialing List Number</li> <li>• Hot Line Destination – Dial Code</li> <li>• Feature Button Assignments 1 - 3</li> <li>• Button types displayed to the Administrator</li> </ul>                                                                                                                                                                                                                                                                                |
| Service Hours Table          | <ul style="list-style-type: none"> <li>• Description</li> <li>• Use time adjustments from location</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Holiday Table                | <ul style="list-style-type: none"> <li>• Name</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Hunt Group                   | <ul style="list-style-type: none"> <li>• Group Name</li> <li>• Group Extension</li> <li>• Group Type</li> <li>• TN</li> <li>• COR</li> <li>• Security Code</li> <li>• ISDN/SIP Caller Display</li> <li>• ACD</li> <li>• Queue</li> <li>• Vector</li> <li>• Coverage Path</li> <li>• Night Service Destination</li> <li>• NM Early Answer</li> <li>• Local Agent Preference</li> <li>• LWC Reception</li> <li>• Audix Name</li> <li>• Message Center</li> <li>• Ignore Call Forwarding</li> <li>• Re-hunt On No Answer (rings)</li> </ul> |

*Table continues...*

| Communication Manager object | Field                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Announcements                | <ul style="list-style-type: none"> <li>• Annc Name</li> <li>• Annc Type</li> <li>• COR</li> <li>• TN</li> <li>• Queue</li> <li>• Rate</li> <li>• Protected</li> <li>• Group/Board</li> </ul> |

 **Note:**

Field-level RBAC is applicable only for the Edit operation.

Field-level RBAC is not applicable when you add Communication Manager objects.

## Endpoints

### Range in endpoints

You can assign a range of values in endpoints and add permissions for specific fields in an endpoint. Specify a definite range, comma separated values, or a single value in the endpoints range field.

For example, you can type 5600:6000 to assign permissions for extensions 5000 to 6000. When you use colon (:) to specify the extension range, the starting and the ending extensions must have the same number of digits.

When you enter comma separated values like 1, 3, 7, 9, and 45, you assign the permissions only to these specified extensions.

 **Note:**

Enter \* in the **Range** field, to assign the permissions for the entire extension range.

- If you assign a specific endpoint range to a user, you can view, add, delete, edit and duplicate only those endpoints within the specified range.
- You can also assign a specific range to the **COR** and **Coverage Path** fields in endpoints.
- You can manage only those endpoint extensions within the specified range.
- For a user, you can assign only those extensions that you specify in the CM Endpoint Communication Profile. For example, if you assign the range 100:200 to user A, and user A

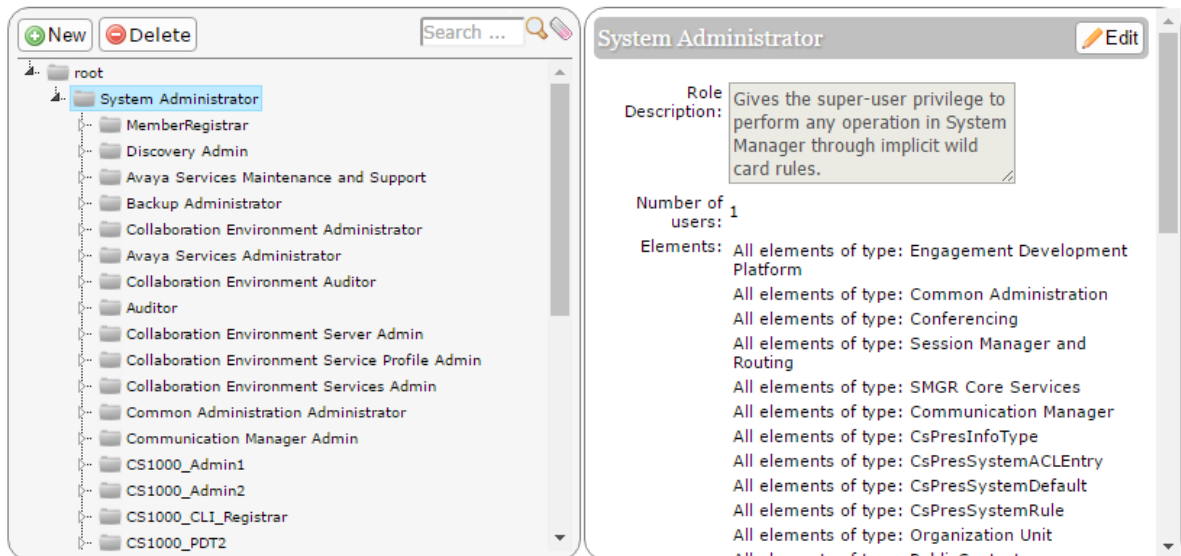
adds an endpoint with extension 201, the system displays an error message and the endpoint add job fails.

## Assigning range for endpoints

### Procedure

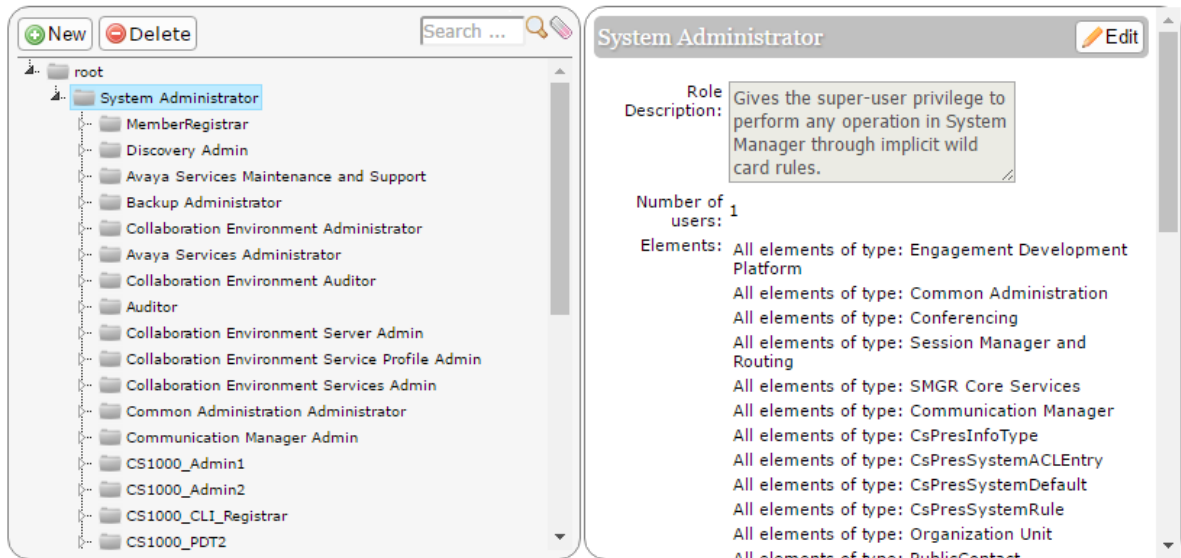
1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. In **Group Name**, select the group of Communication Manager systems to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select any group.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.  
When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Endpoints** permission list by clicking on the arrow next to it. Enter the range you want to specify in the **Extension Range** field.  
You can specify a definite range, enter comma separated values, or a single value in endpoints. For example, 5600:6000, 1, 3, 7, 9, and 45.
18. You can also assign operation permissions like **Bulk Add, Bulk Edit, Delete, Edit, List Usage, Swap, List Trace Station**.  
The user can perform only the actions that are assigned in the operation permissions.
19. Click **Commit**.

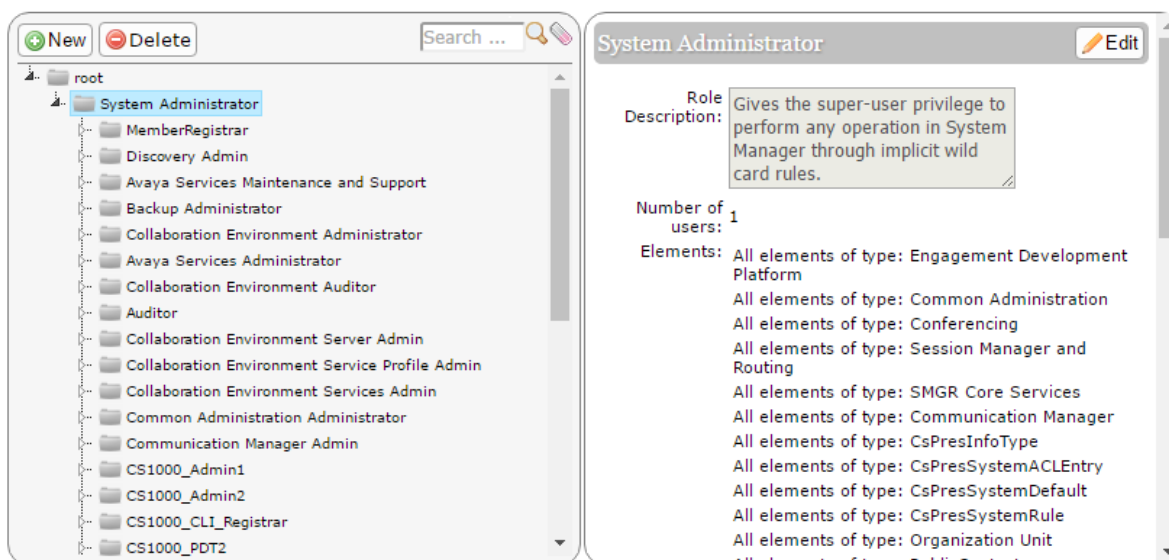
## Assigning permissions for fields in endpoints

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

### Procedure

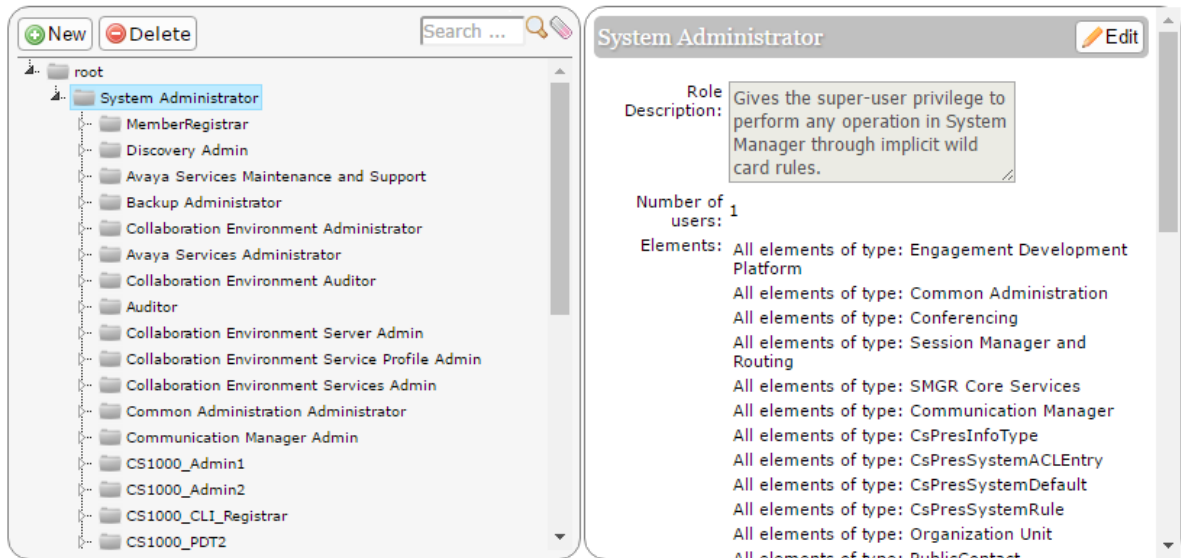
1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. In **Group Name**, select the group of Communication Manager systems to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select any group.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.  
When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand **Endpoint Attributes Permission for Edit Operation** and **Endpoint Buttons Permission for Edit Operation** by clicking on the arrow next to it. Select the buttons and attributes that you want to assign to this role.
18. Click **Commit**.

If you assign this role to a user, the user can edit only the fields that you have assigned in the Permission Mapping page.

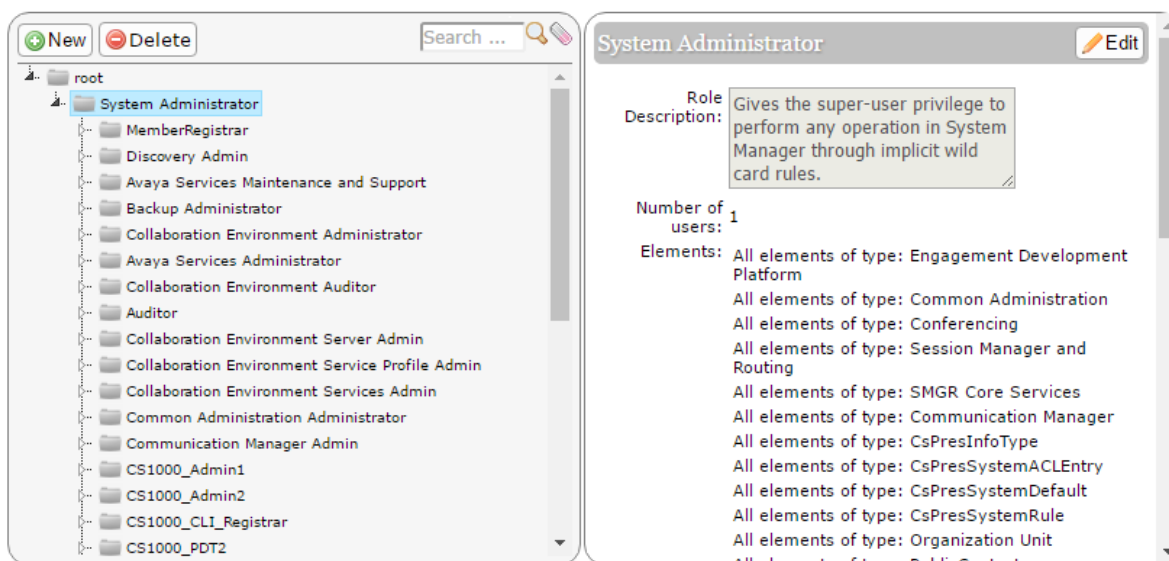
# Hunt Group

## Assigning range for hunt group

### Procedure

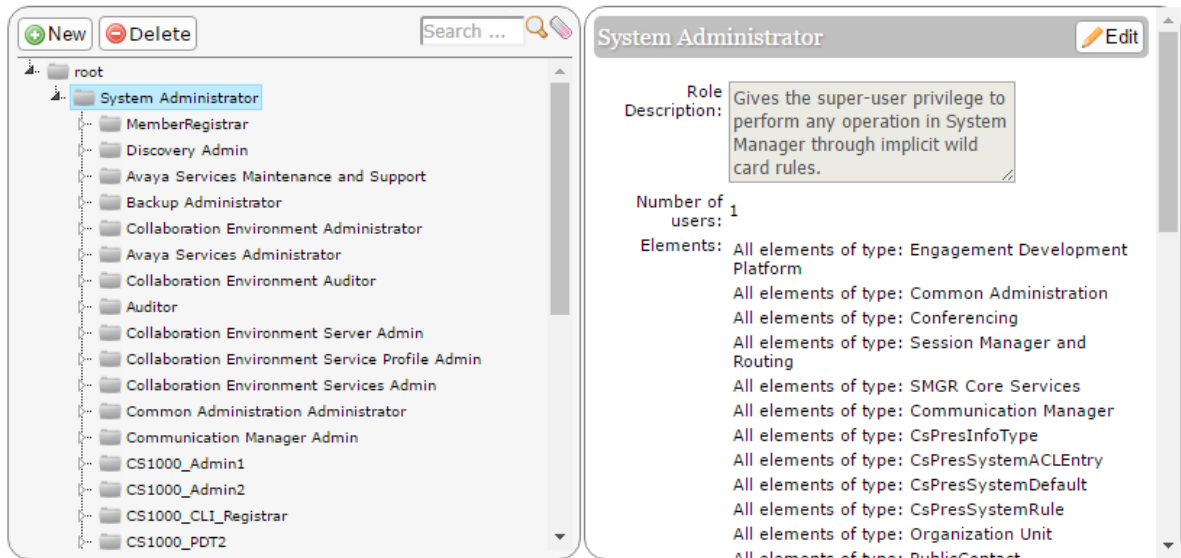
1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. In **Group Name**, select the group of Communication Manager systems to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select any group.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.  
When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Hunt Group** permission list by clicking on the arrow next to it. Enter the range you want to specify in the **Group Number Range** and **Group Extension Range** fields.  
You can specify a definite range, enter comma separated values, or \* for all extensions.
18. You can also assign operation permissions like **Add**, **Edit**, **Delete**, **List Usage**, and **View**.  
The user can perform only the actions that are assigned in the operation permissions.
19. Click **Commit**.



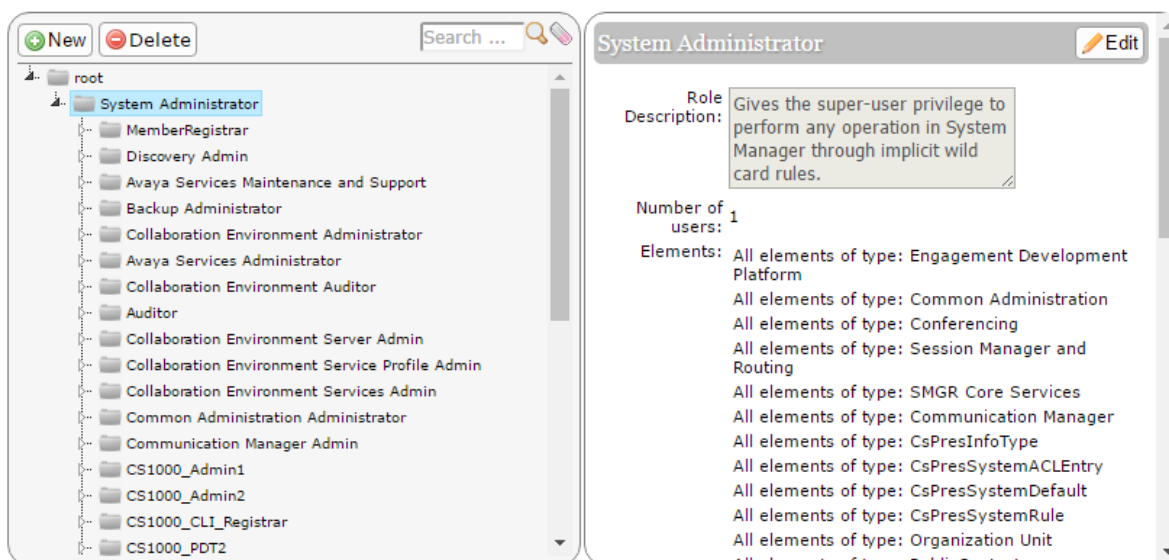
## Assigning permissions for fields in hunt group

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

### Procedure

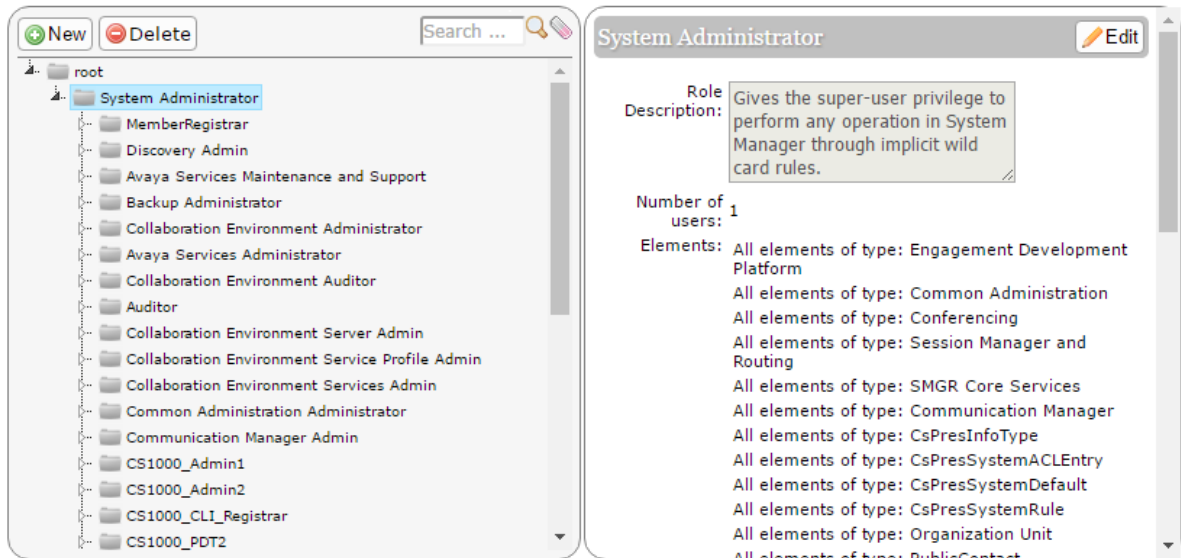
1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. In **Group Name**, select the group of Communication Manager systems to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select any group.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.  
When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Hunt Group Attributes Permission for Edit Operation** list by clicking on the arrow next to it. Select the attributes that you want to assign to this role.
18. Click **Commit**.

If you assign this role to a user, the user can edit only the fields that you have assigned in the Permission Mapping page.

# Trunk Group

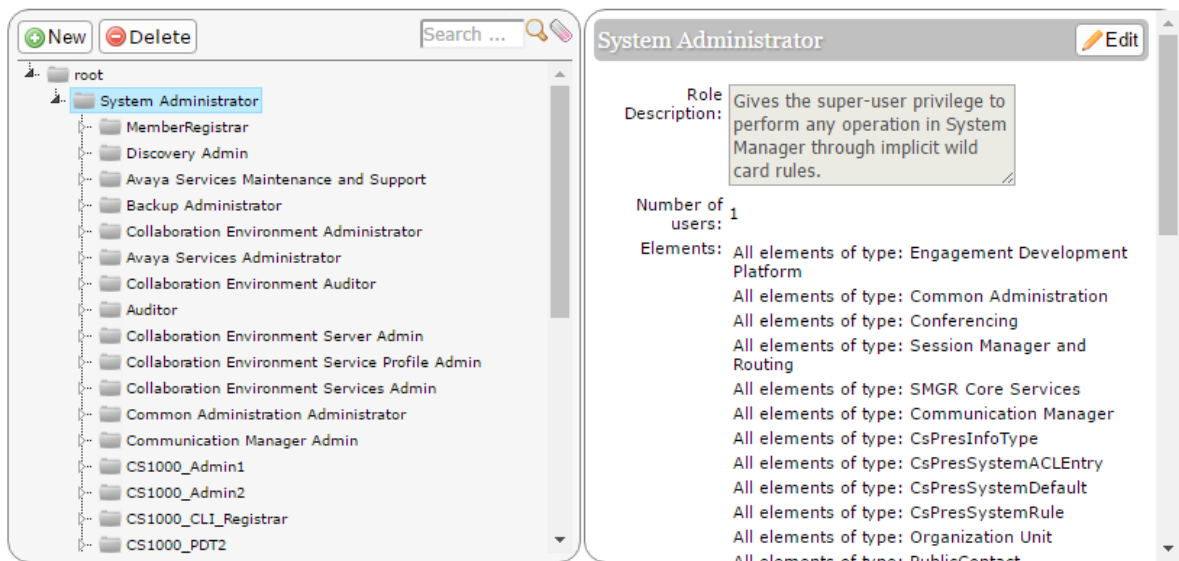
## Assigning permissions for fields in trunk group

Field-level RBAC for Communication Manager objects is applicable only for the edit operation.

### Procedure

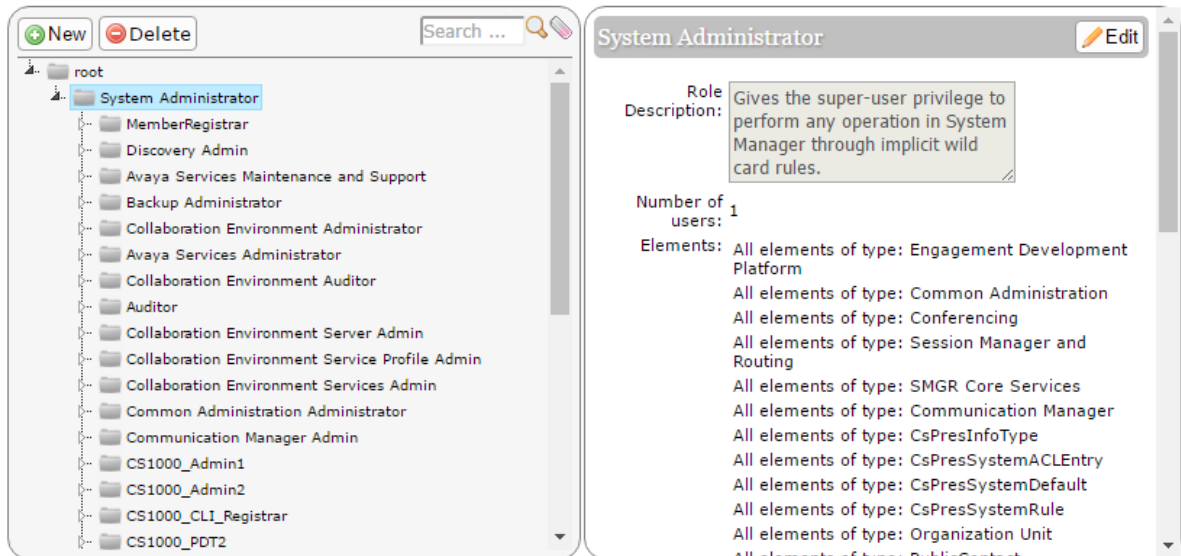
1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping** under **Element/Service Permissions** section.
7. In the **Element or Resource Type** field, click **Communication Manager**.
8. On the Roles page, select an existing role, and do one of the following:
  - Click **New**
  - Right-click and select **New**

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



9. On the Add New Role page, type the name and the description for the role.
10. Click **Commit and Continue**.
11. On the Role Details page, in the **Element/Service Permissions** section, click **Add Mapping**.
12. In the **Element or Resource Type** field, click **Communication Manager**.
13. In **Group Name**, select the group of Communication Manager systems to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select any group.
14. In the **Element or Resource Type** field, click **Communication Manager**.
15. In the **Element or Resource Instance** field, click a Communication Manager instance to which you want to apply this permission.  
When you select **Group Name**, System Manager disables this field.
16. Click **Next**.
17. On the Permission Mapping page, expand the **Trunk Group** permission list by clicking on the arrow next to it. Select the attributes that you want to assign to this role.
18. Click **Commit**.

If you assign this role to a user, the user can edit only the fields that you have assigned in the Permission Mapping page.

# Chapter 7: Managing users, public contacts, and shared addresses

---

## Managing users

---

### Users, public contacts, and shared addresses

#### Manage users

User Management is a shared service that users can gain access from the System Manager web console. User Management supports a logically centralized data store. Applications can gain access to this data store and get the user information that applications need. Administrators or end users do not need to enter user information for each application.

User Management provides administrators with mechanisms to:

- Administer all user attributes, contact information, group membership, user provisioning rule assignment, organization hierarchy assignment, and role assignment, also product-specific user data.
- For each product, extend the underlying user model for product-specific properties, attributes, and any relationship between the attributes.
- Manage specific aspects of user data such as changing a user name or address.

Using User Management, you can:

- Add user profiles.
- View, change, and delete existing user profiles.
- Assign or remove permissions, roles, groups, addresses, and contacts for users.
- Assign user provisioning rule and organization hierarchy.
- Add and change the communication profile of users.
- Change the identity and communication profile data of users in bulk.
- Bulk import users and their attributes, public contact, and shared addresses from an XML file.  
Bulk import users and their attributes from an Excel file.
- Bulk export users and their attributes to an XML and Excel file from the System Manager web console and command line interface.
- Search users.

User Management uses data synchronization to achieve a single-point user administration. User Management synchronizes the user data event that the system generates at the application level with the central user space and other connected applications. If an enterprise directory is connected, then User Management maintains synchronization at the enterprise level. User Management directly adjusts to the changes that occur in the enterprise directory, specifically additions, deletions, and modifications. For more information, see the Directory synchronization overview section.

Roles based access control (RBAC) applies to User Management so that the user role determines the access to user level tasks and access to administrative tasks. Users with login privileges must have permissions to add, change, and delete user accounts on the management console.

To perform the user provisioning by using User Management, map the user to the role with the following permissions:

| Resource type                 | Permissions                 |
|-------------------------------|-----------------------------|
| All elements of type:elements | add, delete, edit, and view |

To perform the user provisioning by using the user provisioning rule, map the user to the role with the following permissions:

| Resource type                 | Permissions |
|-------------------------------|-------------|
| All elements of type:elements | view        |

### Manage public contacts

As an administrator, you can define public contacts of users in System Manager for an enterprise. You can share public contacts by all users in System Manager.

### Manage shared address

All users in the enterprise can share the common addresses called shared address. As an administrator, you can create, change, and delete a shared address of users in the enterprise.

---

## Access to administrative users

Starting from System Manager Release 6.3.8, when you create a role with access to **User Management**, you can restrict the access to the Administrative Users page.

The roles that are created earlier than Release 6.3.8 with permissions to access **User Management** can access the Administrative Users page by default. The roles continue to have permission after the upgrade to Release 6.3.8 or later. To restrict access to the Administrative Users page, clear the **Allow access to Administrative Users Web UI** check box on the Permission Mapping page.

To gain access to the Administrative Users page, log on to the System Manager web console and click the **Users > Administrators** link. The Administrative Users page displays the list of administrative users that are available in the system. By default, when you add user-related permissions to a role, the system selects the **Allow access to Administrative Users Web UI** permission.

---

## End user self provisioning

Using the URL that administrator provides, end users can access the Self Provisioning web interface to change or reset the communication profile password.

End users can start the self provisioning interface from any device that supports a web browser. For example, from a web browser on the computer, mobile phone, and notebook.

By default, **Self Provisioning Status** is set to **true** so that the end user can change the communication profile password.

### Related links

[Disabling self provisioning](#) on page 221

[Generating the communication profile password from the self provisioning interface](#) on page 222

[Changing the communication profile password from the self provisioning interface](#) on page 223

---

## Enabling self provisioning

### About this task

Administrator must disable self provisioning on System Manager for the end user to change the communication profile password.

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR**.
3. On the Edit Profile:SMGR page, set **Self Provisioning Status** to **true**.
4. Click **Commit**.

---

## Disabling self provisioning

### About this task

Administrator must disable self provisioning on System Manager so that the end user cannot change the communication profile password.

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR**.
3. On the Edit Profile:SMGR page, set **Self Provisioning Status** to **false**.

If you set the status to false, the system displays the following message: The provisioning application is currently disabled. Please contact your system administrator.

### Related links

[Generating the communication profile password from the self provisioning interface](#) on page 222

[Changing the communication profile password from the self provisioning interface](#) on page 223

---

## Generating the communication profile password from the self provisioning interface

### About this task

Use this procedure to reset only the Communication Profile password.

### Before you begin

The System Manager administrator must do the following:

- Enable Self Provisioning. For more information, see “Enabling self provisioning”.
- Configure email properties. For more information, see “Configuring email properties”.
- Add the user’s email address in the user profile. For more information, see “User Profile Edit field descriptions”.

### Procedure

1. To gain access to the Self Provisioning web interface, on the web browser, type `https://<IP address of System Manager>/selfprovisioning/`.
2. On the Login page, type the user’s Avaya SIP handle and click **Reset Password**.

#### **Note:**

Avaya SIP handle is in the following format: `handle@domain`.

3. Access the inbox of the email address associated with the provided Avaya SIP handle.
4. In the **Avaya Aura System Manager Password Reset** email, click on the password activation link.

The system sends a new email with a system generated password.

### Next steps

Change the system generated communication profile password. For more information, see “Changing the communication profile password from the self provisioning interface”.

### Related links

[Disabling self provisioning](#) on page 221

[Changing the communication profile password from the self provisioning interface](#) on page 223



---

## Changing the communication profile password from the self provisioning interface

### About this task

Using this procedure, the end user can change the communication profile password from the Self Provisioning web interface.

When the system is overloaded, the Self Provisioning web interface displays the message The Provisioning Application has reached maximum supported load. Please try again after some time.

### Before you begin

The System Manager administrator must Enable Self Provisioning. For more information, see “Enabling self provisioning”.

### Procedure

1. To gain access to the Self Provisioning web interface, on the web browser, type `https://<IP address of System Manager>/selfprovisioning/`.
2. On the Login page, type the user ID and password and click **Login**.

#### **Note:**

- Use the communication address as username and communication profile password or SIP password as password.
  - For users with Communication Manager communication profile, use the Communication Manager extension and security password.
  - Do not leave the user name and password fields blank.
3. On the Password Change for Communication Profile page, in the **Profile Type** field, click one of the following:
    - **SIP**
    - **H.323**
    - **Agent**
    - **Messaging**

### Password Change for Communication Profile

**Profile Type**

**Current Password**

**New Password**

**Confirm New Password**

Submit

Clear

4. Type the current password and the new password, and do one of the following:
  - To clear the values, click **Clear**.
  - To change the password, click **Submit**.

#### Related links

[Disabling self provisioning](#) on page 221

[Generating the communication profile password from the self provisioning interface](#) on page 222

---

## Viewing details of a user

### Before you begin

You require appropriate permissions.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user.
3. To view details of the selected user account, click **View**.

 **Note:**

You can only view details of one user account at a time.

#### Related links

[User Profile | View | <User Name> field descriptions](#) on page 333

## Creating a new user account

You can create new user account using this section or by providing the user provisioning rule.

### Before you begin

- You require permission to add a new user account.
- The role must have the following permissions assigned:

For resource type elements, all permissions in the **Role Resource Type Actions** section.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, click **New**.
3. On the User Profile | Add page, complete the following steps:

- a. **(Optional)** In the **Organization** section, select a tenant from the **Tenant** field.

You must select a tenant only if the user must belong to a tenant.

- b. **(Optional)** On the **Identity** tab, in the Basic Info section, in the **User Provisioning Rule** field, select a user provisioning rule.

You can provide only one user provisioning rule.

#### **Note:**

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

- c. Enter the required information in the remaining fields.

4. Perform one of the following:

- To save the changes, click **Commit**.
- To save the changes and stay on the same page, click **Commit & Continue**.

Before you click **Commit**, ensure that all mandatory fields have valid information.

#### **Important:**

The Communication Manager systems that are undergoing synchronization or are busy, displays the following behavior:

- In Firefox, the system displays the status of the Communication Manager systems that are undergoing synchronization as disabled. The Communication Manager systems are available only after the synchronization is complete. To view the Communication Manager systems, you must start the new user operation again.
- In Internet Explorer, the system does not display the Communication Manager systems that are undergoing synchronization in the list. The Communication

Manager systems are available only after the synchronization is complete. To view the Communication Manager systems, you must start the new user operation again.

#### Related links

[Creating a new user profile using the user provisioning rule](#) on page 226

[User Profile | Add field descriptions](#) on page 295

---

## Creating a new user profile using the user provisioning rule

### Before you begin

Ensure that the role has the following permissions:

For resource type elements, all permissions in the **Role Resource Type Actions** section.

### About this task

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, click **New**.
3. On the User Profile | Add page, complete the following fields:

- **User Provisioning Rule**

You can provide only one user provisioning rule.

- **Last Name**

- **First Name**

- **Login Name**

4. Perform one of the following:

- To save the changes, click **Commit**.
- To save the changes and stay on the same page for making further changes, click **Commit & Continue**.

Before you click **Commit**, ensure that all mandatory fields contain valid information.

The system creates the user with attributes that are defined in the user provisioning rule.

#### Related links

[Creating a new user account](#) on page 225

[User Profile | Add field descriptions](#) on page 295

[Results of using the user provisioning rule](#) on page 227

## Results of using the user provisioning rule

You can expect the following results when you provision the user using the user provisioning rule.

| Provisioning method | Scenario                                                                                                                                                                               | Expected result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User management     | Create user                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                     | The administrator selects the user provisioning rule without adding the communication profile data.                                                                                    | The system displays a warning message. The system applies the user provisioning rule and adds the communication profiles data based on the user provisioning rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                     | The administrator adds the communication profile data, and then selects the user provisioning rule.                                                                                    | The system displays a warning message. The system creates the communication profile based on the user provisioning rule and overwrites the communication profiles data with the data in the user provisioning rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                     | The administrator selects the user provisioning rule. The system populates the communication profile data for the user. The administrator changes the user provisioning rule to blank. | If the user provisioning rule is blank, the system removes all communication profiles that the system used from the user provisioning rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                     | Edit user                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                     | The communication profile data already exists for the user that was created using the user provisioning rule, and the administrator selects a different user provisioning rule.        | <p>The system displays an error message if a communication profile exists for the user and the same profile is present in the user provisioning rule that you select.</p> <p>If there are no conflicts in the communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select.</p> <p>For example, the user has the Session Manager communication profile that is created using a user provisioning rule, and the administrator selects a different user provisioning rule that has the Communication Manager communication profile. The user now has the Communication Manager and Session Manager communication profiles.</p> |

*Table continues...*

| Provisioning method | Scenario                                                                                                                                                                                        | Expected result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | The communication profile data that is created without the user provisioning rule exists for the user. The administrator selects the user provisioning rule.                                    | <p>The system displays an error message if a communication profile exists for the user and the same profile is present in the user provisioning rule that you select.</p> <p>If there are no conflicts in the communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select.</p> <p>For example, the user has the Session Manager communication profile and the user provisioning rule that is created with Communication Manager communication profile. When the administrator uses the user provisioning rule, the user contains the Communication Manager and Session Manager communication profiles.</p> |
|                     | The administrator sets the user provisioning rule to blank in the Edit User page.                                                                                                               | The system disassociates the user provisioning rule with the user. The communication profiles created using the user provisioning rule remain unchanged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Bulk import         | Create user                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                     | The administrator creates the user using the bulk import feature from the XML or Excel file. The XML or Excel file contains the user provisioning rule without the communication profile data.  | The system applies the user provisioning rule and populates the communication profiles provided in the user provisioning rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                     | The administrator creates the user using the bulk import feature from the XML or Excel file. The XML or Excel file contains the user provisioning rule with the communication profile data.     | <p>The communication profile data in the XML or Excel file takes precedence over the user provisioning rule.</p> <p>The system uses the user provisioning rule only for the communication profile that is not present in the XML or Excel file.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                     | Edit user                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                     | <p>The communication profile data that is created using the user provisioning rule exists for the user.</p> <p>In bulk import, the user provisioning rule is not mentioned in the XML file.</p> | The system disassociates the user provisioning rule with the user. The communication profiles in the Merge and Replace option with the Complete and Partial Import type remain unchanged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table continues...

| Provisioning method       | Scenario                                                                                                                                                                                                                                                                             | Expected result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | The communication profile data that is created without the user provisioning rule. The user provisioning rule is mentioned in the XML file.                                                                                                                                          | <p>The user import operation fails if any communication profile exists for the user and the same is present in the user provisioning rule provided in XML.</p> <p>If there are no conflicts in the communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you provided in XML.</p> <p>For example, the user has the Session Manager communication profile that is created using a user provisioning rule, and the administrator selects a different user provisioning rule that has the Communication Manager communication profile. After import, the user contains the Communication Manager and Session Manager communication profiles.</p> |
|                           | <p> <b>Note:</b></p> <p>You cannot select a different user provisioning rule for partial import. Use the complete XML import with Merge or Replace option to change the user provisioning rule.</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Directory synchronization | Create user                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                           | The user provisioning rule is configured in the LDAP mapping.                                                                                                                                                                                                                        | The system applies the user provisioning rule and populates the communication profiles provided in the user provisioning rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                           | Edit user                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                           | The communication profile that is created using the user provisioning rule exists for the user. The value of the user provisioning rule is changed in LDAP.                                                                                                                          | <p>User synchronization fails if the communication profile exists for the user and the same profile is present in the new user provisioning rule that is configured in LDAP.</p> <p>If no conflicts in communication profile, then the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select.</p>                                                                                                                                                                                                                                                                                                                                                             |

Table continues...

| Provisioning method | Scenario                                                                                                                                                             | Expected result                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | The user provisioning rule is not associated with the existing user. The new user provisioning rule values are configured in LDAP for the user.                      | User synchronization fails if the communication profile exists for the user and the same profile is present in the new user provisioning rule that is configured in LDAP.<br><br>If no conflicts in communication profile, the system merges the communication profile with the existing communication profile and the new user provisioning rule that you select. |
|                     | The communication profile that is created using the user provisioning rule exists for the user, and the value of the user provisioning rule is set to blank in LDAP. | The system disassociates the user provisioning rule with the user. The communication profiles that are created using the user provisioning rule remain unchanged.                                                                                                                                                                                                  |

## Modifying user accounts

### Before you begin

- You require permissions to modify the user details. If you select a user that does not have the permission to modify the details, the system does not display the **Edit** button.
- The role must have the following permissions assigned:  
For resource type elements, all permissions in the **Role Resource Type Actions** section.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user.

#### **Note:**

At one time, you can edit only one user account.

3. To edit a user account, click one of the following:
  - **Edit**.
  - **View > Edit**.
4. On the User Profile | Edit | <User Name> page, do the following:
  - a. **(Optional)** In the **Organization** section, select a tenant from the **Tenant** field.  
You must select a tenant only if the user must belong to a tenant.
  - b. **(Optional)** On the **Identity** tab, in the Basic Info section, in the **User Provisioning Rule** field, select a user provisioning rule.  
You can provide only one user provisioning rule.



 **Note:**

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

- c. Enter the required information in the remaining fields.

For information, see “User Profile | Edit | <User Name> field descriptions”.

- You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.
- If you must change the tenant, delete the user and associate the user with the tenant.
- System Manager does not automatically modify the user if the user provisioning rule changes.
- You can select a different user provisioning rule when you modify the user information.

 **Note:**

You can associate the user to an existing tenant.

5. Perform one of the following:

- To save the changes, click **Commit**.
- To save the changes and stay on the same page, click **Commit & Continue**.

### Related links

[User Profile | Edit | <User Name> field descriptions](#) on page 315

[Results of using the user provisioning rule](#) on page 227

---

## Creating duplicate users

You can duplicate the user details to create a new user account by copying information from an existing user account. Using the Duplicate feature, you cannot copy the confidential information, such as addresses, private contacts and associated contacts in the contact list, password, and login name of the user.

Using the Duplicate feature, you can also copy the communication profiles like CM Endpoint and Session Manager. However, you cannot copy CS 1000 Endpoint Profile. You must add the CS 1000 Endpoint Profile after you create a duplicate user.

### Before you begin

You require permission to copy the user details.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.

2. On the Manage Users page, select the user account that you must duplicate.
3. Click **Duplicate**.
4. On the User Profile | Duplicate | <User Name> page, enter the appropriate information.
5. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

---

## Removing user accounts

### About this task

When you remove a user, the system marks the user as deleted and saves the user in a list of deleted users. The system removes the roles associated with the user. However, the contacts, addresses, and communication profiles of the user still exist in the database. You can permanently remove the deleted users from the database.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select one or more users from the table, and click **Delete**.
3. On the User Delete Confirmation page, click **Delete**.

#### **Note:**

You cannot delete users:

- With the login name *admin* from the Manage Users page.
- Synchronized from LDAP.

### Related links

[Removing the deleted users from the database](#) on page 232

---

## Removing the deleted users from the database

Using this procedure, you can permanently delete a user from the database.

### Before you begin

Ensure you have the permission to delete the selected user.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, click **More Actions > Show Deleted Users**.
3. On the Show Deleted Users page, select the users to delete, and click **Delete**.

4. On the User Delete Confirmation page, click **Delete**.

#### Related links

[Removing user accounts](#) on page 232

---

## Editing users in bulk

### About this task

On the System Manager web console, you can change the identity and communication profile data of users in bulk.

#### **Note:**

With **Bulk Edit Users**, you can select multiple users and create or update the communication profile data for the users. However, you cannot delete communication profiles.

While performing bulk edit operation, you do not validate the details of the users because bulk operation impacts all users.

You can schedule the bulk edit job to run at a later time.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. Select one or more users and click **More Actions > Bulk Edit Users**.
3. On the User Bulk Editor page, in the **Basic** and **Communication Profile** tabs, change the fields as appropriate.  
  
When you provide the communication profile password during the bulk edit of users, the system overwrites the existing communication profile password of the user.
4. Click **Run Now** or **Schedule**.
5. To view the status of the bulk edit job, click **More Actions > Status of Bulk Edit Users Jobs**.

For more information, see Viewing bulk user edit jobs.

#### Related links

[User Bulk Editor field descriptions](#) on page 235

---

## Viewing bulk user edit jobs

### Before you begin

Create a bulk user edit job and run the job.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.

2. Click **More Actions > Status of Bulk Edit Users Jobs**.
3. On the Schedule Bulk Edit of Users page, select a bulk edit job and click **View**.  
The system displays job details on the Bulk Edit Job Details page.
4. To view any latest changes in job details, click **Refresh**.

---

## Deleting the bulk user edit job

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. Click **More Actions > Status of Bulk Edit Users Jobs**.
3. On the Schedule Bulk Edit of Users page, select one or more bulk edit jobs and click **Delete**.
4. On the Filter Profile Delete Confirmation page, click **Delete**.

The system deletes the bulk edit job.

---

## Create new profile option

During add and edit profile operations, based on the selection of the **Create New Profile if it doesn't exist for the user** check box and the availability of the communication profile, System Manager provides the following:

| Create New Profile if it doesn't exist for the user check box | Communication profile | Add operation                                                        | Edit operation                                                              |
|---------------------------------------------------------------|-----------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Selected                                                      | Exists                | You cannot update the existing communication profile.                | The profile remains unchanged.                                              |
| Selected                                                      | Does not exist        | The system creates the communication profile.                        | The profile remains unchanged.                                              |
| Not selected                                                  | Exists                | The communication profile that is already created remains unchanged. | The system updates the communication profile based on the changes you make. |
| Not selected                                                  | Does not exist        | No change because you have not selected the check box.               | No change. You cannot update a communication profile that does not exist.   |

## User Provisioning Rules and User Bulk Editor

You can edit the users in bulk from one of the following:

- On the User Provisioning Rules page, from the **User Provisioning Rule** link. For more information, see [User Provisioning Rule field descriptions](#) on page 619.
- On the User Bulk Editor page, from the **User Management > Manage Users > More Actions > Bulk Edit Users** link. For more information, see [User Bulk Editor field description](#) on page 235.

## User Bulk Editor field descriptions

### Basic

 **Note:**

On the **Basic** tab, when you provide the value in a field, the system applies the same value for all selected users.

| Name                                                | Description                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP Domain</b>                                   | <p>The name of the configured SIP domain name.</p> <p>If <b>SIP Domain</b> is nonblank, create an Avaya SIP communication address for the user.</p> <p>The system changes the SIP domain for all selected users with the value that you provide in this field.</p>                                     |
| <b>Presence/IM Domain</b>                           | <p>The name of the configured Presence domain name.</p> <p>If <b>Presence/IM Domain</b> is nonblank, create an Avaya Presence/IM communication address for the user.</p> <p>The system changes the Presence/IM Domain domain for all selected users with the value that you provide in this field.</p> |
| <b>Auto Generate Communication Profile Password</b> | <p>The option to automatically generate the communication profile password.</p> <p>If you select the <b>Auto Generate Communication Profile Password</b> option, the system disables the <b>Communication Profile Password</b> field.</p>                                                              |

*Table continues...*

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Communication Profile Password</b>                 | <p>The communication profile password.</p> <p>The field is available only if you enable the communication profile. The password policy is configured on the <b>Users &gt; User Management &gt; Communication Profile Password Policy</b> page.</p> <p>When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user.</p>                                                                                      |
| <b>Edit</b>                                           | <p>The link to change the Communication Profile password.</p> <p>When you click the <b>Edit</b> link, the system displays the <b>Confirm Password</b> field along with the <b>Generate</b> and <b>Cancel</b> links.</p>                                                                                                                                                                                                                                                                                     |
| <b>Confirm Password</b>                               | The communication profile password that you reenter for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Generate</b>                                       | <p>The option to automatically generate the communication profile password.</p> <p>System Manager sends the generated password to the user, if:</p> <ul style="list-style-type: none"> <li>• Email configuration properties are set on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR</b> page.</li> </ul> <p>For more information, see “Configuring email properties”.</p> <ul style="list-style-type: none"> <li>• <b>Email Address</b> is configured on the <b>Identity</b> tab.</li> </ul> |
| <b>Cancel</b>                                         | Cancels the password change operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Prefix for Avaya E164 Handle</b>                   | The digits that the system must prefix to the telephone number or Avaya E.164 handle. The default is plus (+).                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Language Preference</b>                            | The preferred written or spoken language of the user. For example, English.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Time Zone</b>                                      | The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Allow H.323 and SIP Endpoint Dual Registration</b> | <p>The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</p>                                                                                                                            |

## Communication Profile: Session Manager Profile

**\* Note:**

The system displays the following fields only if a communication profile of the user exists for the product:

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Session Manager</b>   | The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura <sup>®</sup> network. You must select the primary Session Manager server. |
| <b>Secondary Session Manager</b> | The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.                                                                                                             |

*Table continues...*

| Name                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Survivability Server</b>                                     | <p>For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.</p> <p> <b>Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.</p> <p>After typing minimum of 3 characters, wait for three seconds to capture the final keyword, and fetch the required results.</p> |
| <b>Max. Simultaneous Devices</b>                                | <p>The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Block New Registration When Maximum Registrations Active</b> | <p>If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.</p> <p> <b>Note:</b></p> <p><b>Block New Registration When Maximum Registrations Active</b> is available only when you select the <b>Create New Profile if it doesn't exist for the user</b> check box while creating the user profile.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

*Table continues...*



| Name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Origination Application Sequence</b> | <p>The application sequence that the system invokes when routing calls from this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> |
| <b>Termination Application Sequence</b> | <p>The application sequence that is invoked when the system routes calls to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> |
| <b>Home Location</b>                    | <p>The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any location. You must specify a value.</p>                                                                                                                                                                        |
| <b>Conference Factory Set</b>           | <p>The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.</p> <p>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.</p>                                                                                                                                                                 |

### Communication Profile tab: Avaya Breeze® platform Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

| Name                   | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Service Profile</b> | The profile that you assign to the user. The user can gain access to the service contained in the profile. |

### Communication Profile: CM Endpoint Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

By default, the system displays only **Profile Type**, **Template**, **Security Code**, and **Preferred Handle** fields. The system displays the remaining fields only when you select the **Create New Profile if it doesn't exist for the user** check box while creating the communication profile.

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use Next Available Extension</b> | <p>The option to instruct the system to create a new extension for the user.</p> <p> <b>Note:</b></p> <p>For LDAP synchronization, the value in the <b>Use Phone Number last ..... digits for Extension</b> field takes priority.</p>                                                                      |
| <b>Template</b>                     | The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add.                                                                                                                                                                                                                                                        |
| <b>Sub Type</b>                     | This field is configured for CS 1000 station types only. You can select the specific set for <b>Set Type</b> . On the Manage Endpoint page, <b>Sub Type</b> is labeled as <b>Set</b> .                                                                                                                                                                                                        |
| <b>System ID</b>                    | <p>This field is configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0 more than one station can use the combination of <b>System ID</b> and <b>Terminal Number</b>.</p> <p>With Release 8.0.1, each station must have a unique combination of <b>System ID</b> and <b>Terminal Number</b>.</p> |
| <b>Security Code</b>                | The security code for authorized access to the endpoint.                                                                                                                                                                                                                                                                                                                                      |

*Table continues...*

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Preferred Handle</b>                               | Avaya SIP or Avaya E.164 handle that is administered for the user. The field is optional. By default, the field is blank.                                                                                                                                                                                                                                                  |
| <b>Password</b>                                       | The password to gain access to the endpoint.<br><br>The system displays the field if you select <b>Agent</b> in <b>Profile Type</b> .                                                                                                                                                                                                                                      |
| <b>Allow H.323 and SIP Endpoint Dual Registration</b> | The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a> . |

### Communication Profile: CS 1000 Endpoint Profile

The communication profile is available only for creating a user profile.

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | An option to create the profile for the user if a profile does not already exist.<br><br>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.<br><br>For more information, see <a href="#">Create new profile option</a> on page 234. |

| Name                                                     | Description                                                                                                                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                            | The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.                                  |
| <b>Target</b>                                            | The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. |
| <b>Template</b>                                          | The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. |
| <b>Include in Corporate Directory</b>                    | The option to add this profile to the CS 1000 Corporate Directory feature.                                                                |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | An option to specify whether to delete the endpoint from the CS 1000 system when you unassign the endpoint from the user.                 |

## Communication Profile: Messaging Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

By default, the system displays only **Template** and **Password** fields. The system displays the remaining fields only when you select the **Create New Profile if it doesn't exist for the user** check box while creating the communication profile.

| Name                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                                                  | The messaging system on which you add the subscriber. You must select the system.                                                                                                                                                                                                                                                                                                 |
| <b>Mailbox Number</b>                                                          | <p>The mailbox number of the subscriber. The options are:</p> <ul style="list-style-type: none"> <li>• Use CM Extension: Use this option only if the Communication Manager profile and Session Manager profile are specified.</li> <li>• Use Next Available Subscriber: Use this option if the system must use the next mailbox number to associate with this profile.</li> </ul> |
| <b>Template</b>                                                                | The system-defined or user-defined template that you associate with the subscriber.                                                                                                                                                                                                                                                                                               |
| <b>Password</b>                                                                | The password for logging in to the mailbox. You must provide the password.                                                                                                                                                                                                                                                                                                        |
| <b>Delete Subscriber on Unassign of Subscriber from User or on Delete User</b> | The option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this Messaging profile or delete the user.                                                                                                                                                                                            |

## Communication Profile: Avaya Messaging Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

| Name                              | Description                                                                                                                                                                                                                                                                               |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                     | The Avaya Messaging system to which you add a mailbox.                                                                                                                                                                                                                                    |
| <b>Refresh</b>                    | <p>The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use.</p> <p>You do not require to refresh for every user.</p>                                                                          |
| <b>Use Next Available Mailbox</b> | The option to specify if the system must use the next mailbox number to associate with this profile.                                                                                                                                                                                      |
| <b>Mailbox Range</b>              | <p>The range of mailbox numbers assigned to the Avaya Messaging system.</p> <p> <b>Note:</b></p> <p>This option is available only when you select the <b>Use Next Available Mailbox</b> check box.</p> |
| <b>Numeric Password</b>           | The numeric password that is used to log in to the Avaya Messaging system.                                                                                                                                                                                                                |
| <b>Application User Password</b>  | The password that is used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.                                                                                                                                           |
| <b>Company</b>                    | The name of the company to which the user belongs.                                                                                                                                                                                                                                        |
| <b>Department</b>                 | The department to which the user belongs.                                                                                                                                                                                                                                                 |
| <b>Feature Group</b>              | The feature group name that determines the rules for the mailboxes associated with it.                                                                                                                                                                                                    |

*Table continues...*

| Name                             | Description                                                                                                                                                                                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Capability</b>                | <p>The type of functionality that the user contains. The values are:</p> <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Fax</b></li> <li>• <b>Messaging</b></li> <li>• <b>Collaboration</b></li> <li>• <b>Messaging and Collaboration</b></li> </ul> |
| <b>Domain Account Name</b>       | <p>The mailbox NT account name for the Avaya Messaging profile. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Same as Login Name</b></li> <li>• <b>Admin Specified</b></li> </ul>                                                                         |
| <b>Synchronization User Name</b> | <p>The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Same as Login Name</b></li> <li>• <b>Admin Specified</b></li> </ul>           |

### Communication Profile tab: Presence Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

| Name          | Description                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b> | <p>The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile:</p> <ul style="list-style-type: none"> <li>• Aggregate presence</li> <li>• Archive instant messages if the Instant Messages option is enabled</li> </ul> |

*Table continues...*

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP Entity</b>                          | The option to route the SIP-based messages through Presence Services.<br><br>This system selects the SIP entity only if you select a Presence Services instance in the <b>System</b> field. <b>SIP Entity</b> is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.                                                         |
| <b>IM Gateway SIP Entity</b>               | The Presence Services instance for the user.                                                                                                                                                                                                                                                                                                                                            |
| <b>Publish Presence with AES Collector</b> | The option that determines if Presence Services must publish presence with AES Collector. The options are: <ul style="list-style-type: none"> <li>• <b>System Default</b></li> <li>• <b>Off</b></li> <li>• <b>On</b></li> </ul> The default is <b>System Default</b> . You can change the default value. You do not require to configure AES Collector in the Presence Services server. |

### Communication Profile: IP Office Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | An option to create the profile for the user if a profile does not already exist.<br><br>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.<br><br>For more information, see <a href="#">Create new profile option</a> on page 234. |

By default, the system displays only **Extension**, **Template**, and **Set Type** fields. The system displays the remaining fields only when you select the **Create New Profile if it doesn't exist for the user** check box for creating the communication profile.

| Name             | Description                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>    | The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.                                                                                                                                                                                                               |
| <b>Extension</b> | The extension of the endpoint to which you associate the profile. The options are: <ul style="list-style-type: none"> <li>• Use CM Extension: Use this option only if Communication Manager profile is specified.</li> <li>• Use Next Available Extension: Use this option if the system must use the next extension to associate with this profile.</li> </ul> |

*Table continues...*

| Name            | Description                                                                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Template</b> | A list of user templates from which you can select a template to set the user configurations.                                                                                        |
| <b>Set Type</b> | The set type for the IP Office endpoint profile. By default, the <b>Set Type</b> field is disabled. If you select a template, the system automatically populates the set type value. |

### Communication Profile: Conferencing Profile

The communication profile is available only for creating a user profile.

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |

| Name                                                          | Description                                                                                                                                                                                              |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Template</b>                                               | The template that you use to set the user configurations.                                                                                                                                                |
| <b>Location</b>                                               | <p>The location that Conferencing uses when the IP address of the calling phone does not match the IP address pattern of any location.</p> <p>The field is used to support the mobility of the user.</p> |
| <b>Select Auto-generated Code Length</b>                      | The number of digits in the security code that the system generates.                                                                                                                                     |
| <b>Auto Generate Participant and Moderator Security Codes</b> | The option to instruct the system to generate the security codes for the participant and moderator.                                                                                                      |

### Communication Profile tab: Equinox Profile

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create New Profile if it doesn't exist for the user</b> | <p>An option to create the profile for the user if a profile does not already exist.</p> <p>The system displays the check box only when you select the communication profile. If the communication profile already exists, the system does not make any changes to the profile data.</p> <p>For more information, see <a href="#">Create new profile option</a> on page 234.</p> |



| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Equinox User Password</b> | The password that is used to log in to the Avaya Workplace Client Management.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Virtual Room Number</b>   | <p>The number of a virtual room that is used to create a conference.</p> <p>By default Virtual Room Number serves as Meeting ID when a conference is created. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Use Phone Number:</b> This will use Communication Manager extension. Use this option only if Communication Manager profile is already associated with the user or being associated with the user.</li> <li>• <b>Auto Generate Virtual Room Number:</b> Use this option if the system needs to generate the Virtual Room Number automatically.</li> </ul> |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Run Now</b>  | Runs the bulk user edit job immediately.                            |
| <b>Schedule</b> | Schedules the bulk user edit job.                                   |
| <b>Cancel</b>   | Cancels the edit operation and returns to the User Management page. |

## Related links

[Create new profile option](#) on page 234

## Filtering users

### About this task

You can apply filter to the following user information:

- First Name
- Surname
- Display Name
- Login Name
- SIP Handle

You can apply one or more filters to view users that match the filter criteria. Table filter works based on “starts with” mechanism.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.

2.

On the Manage Users page, click the **Filter menu** icon  displayed next to the column according to which you want to filter.

3. Enter the information for one or more of the following filter criteria:

- To filter users by the first name, in the **First Name** column, enter the first name of the user.  
To filter names that begin with a specific letter, enter the letter in the field. You can enter a string of letters to filter the names that begin with the string.
- To filter users by the surname, in the **Surname** column, enter the last name of the user.
- To filter users by the display name, in the **Display Name** column, enter the display name of the user.
- To filter users by the login name, in the **Login Name** column, enter the login name.  
To filter the login names that begin with a specific letter, enter the letter in the field. You can enter a string of letters to filter login names that begin with the string.
- To filter users by the SIP handle, in the **SIP Handle** column, enter the SIP handle (E.164 handle and Avaya SIP Handle) of the user.

4. **(Optional)** To hide the column filters, click **Disable**.

This action does not clear any filter criteria that you had set.

5. Press Enter from keyboard to apply filters.

The table displays the users that match the filter criteria.

6.

To clear the filter criteria, click the **Clear Filter** icon  displayed on the lower-right corner of the table.

## User searchable fields

System Manager supports user search for **User Management** objects.

The following table lists the user searchable fields in the search component:

| User Management object | Field Names                                                                               | Supported Actions  |
|------------------------|-------------------------------------------------------------------------------------------|--------------------|
| User                   | User Name, First Name, Last Name, Display Name, Endpoint Display Name, Login Name, Handle | View, Edit, Delete |

### \* Note:

- In the **Search** component, you can find a user match only when the searchable field starts with the search query.

- For handle search, all the handles get concatenated in one string. If you have multiple handles, you can only search using the start of the first handle string.

For information about the search component, see “Search component for Communication Manager objects”.

---

## Searching for users by using Search component

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. In the **Search** component, at the top of the **Manage Users** page, search for users.

---

## Searching for users by using Advanced Search

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, click **Options > Advanced Search** on the upper-right corner of the page.
3. In the Criteria section, do the following:
  - a. In the first field, select the operator.

**Note:**

This field appears dimmed if there is only one search criteria section.

  - b. In the second field, select the search criterion.
  - c. In the third field, enter the condition.
  - d. In the fourth field, enter the search value.
4. To add another search criterion, click plus (+) and repeat Step 3a through Step 3d.  
To delete a search criterion, you must click the **Delete** icon. The system displays this icon when more than one search criterion is available.
5. Click **Apply Filter**.  
The **Users** table lists the users that match the search criteria.

---

## Assigning roles to a user

To provide access to resources, you must assign roles to users. Use this procedure to assign an admin role to an end user. You can assign up to 20 roles per user.

You can also assign roles to users by using the Roles page, on the System Manager web console. During the tenant administration, the **Membership** tab is unavailable for the tenant administrator.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, perform one of the following:
  - To assign roles while setting up a new user account, click **New**.
  - To assign roles to an existing user, select the user and click **Edit** or **View > Edit**.
3. On the User Profile | Edit | <User Name> or User Profile | Add page, click the Membership tab.
4. Click **Assign Roles**.
5. In the Assign Roles section, select the roles.
6. To assign the roles to the selected user, click **Select**.
7. On the User Profile | Edit | <User Name> or User Profile | Add page, click **Commit**.

#### **Note:**

- For a new user, if you assign a role other than the End-User role, the system prompts for the password.
- For an existing user, the system resets the password to match the login name of the user when you:
  - Change the login name.
  - Assign a role other than End-User role and you do not provide a new password.

When the user logs in, the system prompts the user to change the password on the next login.

---

## Assigning roles to multiple users

To provide access to resources, you must assign roles to the user accounts. Use this procedure to assign admin role to an end user.

You can also assign roles to the users using the Roles service provided by System Manager. To access the Roles service, click **Groups & Roles > Roles**.

During the tenant administration, the **Membership** tab is unavailable for the tenant administrator.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select the users and click **More Actions > Assign Roles**.
3. On the Assign Roles page, select the roles from the **Available Roles** section.

4. Click **Commit** to assign the roles to the selected users.

---

## Removing roles from a user

### Before you begin

You must have permissions to remove the roles for the user.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Membership** tab.
4. Select the roles you want to remove and click **UnAssign Roles**.

You can also assign roles to users using the Roles functionality in System Manager. To access Roles, on the System Manager console, click **Groups & Roles > Roles**

5. Click **Commit** to save the changes.

 **Note:**

You can also assign roles to users using the Roles functionality in System Manager. To access Roles, on the System Manager console, click **Groups & Roles > Roles**.

6. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

---

## Assigning groups to a user

You can also assign groups to users using the groups functionality in System Manager. To gain access to **Groups**, on System Manager web console, click **Groups & Roles > Groups**.

During the tenant administration, the **Membership** tab is unavailable for the tenant administrator.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, perform one of the following steps:
  - To assign groups while setting up a new user account, click **New**.
  - To assign groups to an existing user, select the user and click **Edit**.
3. On the User Profile | Edit | <User Name> page or the User Profile | Add page, click the **Membership** tab.
4. In the Group Membership section, click **Add To Group**.

5. On the Assign Groups page, select the groups from the **Available Groups** section.
6. Click **Select** to assign the groups to the user.
7. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

---

## Assigning groups to multiple users

You can also assign groups to users using the groups functionality in System Manager. To access **Groups**, on System Manager web console, click **Groups & Roles > Groups**.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select the users and click **More Actions > Add To Group**.
3. On the Add to Group page, select the groups from the **Available Groups** section.
4. Click **Commit** to assign groups to the selected users.

---

## Removing a user from groups

You can also assign groups to users using the groups functionality in System Manager. To access **Groups**, on System Manager web console, click **Groups & Roles > Groups**.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, perform one of the following steps:
  - To remove a group in the edit mode, select the user and click **Edit**.
  - To remove a group in the view mode, select the user and click **View > Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Membership** tab.
4. In the Group Membership section, select the groups from which you want to remove the user and click **Remove From Group**.
5. Click **Commit** to save the changes.

---

## Viewing deleted users

### About this task

When you remove a user from the Manage Users page by using the **Delete** option, the system temporarily removes and stores the user in the **Deleted Users** table.

## Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, click **More Actions > Show Deleted Users**.

On the Soft Deleted Users page, the system displays the temporarily deleted users in the Deleted Users table.

---

## Restoring a deleted user

### About this task

Use this procedure to restore a user that you deleted by using the **Delete** option on the Manage Users page.

### Before you begin

Ensure that you have permission to restore the selected deleted user.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, click **More Actions > Show Deleted Users**.
3. On the Soft Deleted Users page, select the user that you want to restore, and click **Restore**.
4. On the User Restore Confirmation page, click **OK**.
5. Click **Commit**.

#### **Note:**

For a restored user, if you assign a role other than End-User, the system prompts for a password.

---

## Assigning users to roles

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. From the list of roles, click the name of the role.
4. On the **Assigned Users** tab, click **Select Users**.

The system displays the list of users.

5. Select the users and click **Commit**.

---

## Unassigning users from role

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select a role and click **Edit**.
4. On the Role Details page, click the **Assigned Users** tab.
5. Click **Selected Users**.
6. On the Assigned Users page, clear the check box of the user whom you want to unassign.
7. Click **Commit**.

---

## Managing addresses

### Adding a user address

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, do one of the following:
  - To add an address for a new user account, click **New > Identity > Address > New**.
  - To add a new address for an existing user, select the user and click **Edit > Identity > Address > New**.
3. On the Add/Edit Address page, enter the address details.
4. Click **OK** to add the address.
5. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

#### Related links

[Add Address field descriptions](#) on page 256

### Editing an address

#### About this task

Use this procedure to modify the address of a user. Note that you cannot edit a shared address.

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.



2. On the Manage Users page, select a user, and click **Edit > Identity > Address**.
3. In the **Address** area, select the mailing address that you want to modify and click **Edit**.

You cannot modify a shared address by using this feature.

4. On the Add/Edit Address page, modify the information.
5. Click **OK**.
6. Click **Commit**.

## Deleting an address

### About this task

Use this procedure to delete a private mailing address from the database.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. Do one of the following :
  - If you are on the User Profile | Add page or on the User Profile | Duplicate | <User Name> page and have added an address, then navigate to **Identity > Address**.
  - On the Manage Users page, select a user and click **Edit > Identity > Address**.

3. Select the address that you want to delete and click **Delete**.

If the address that you delete is a shared address, the system removes the address from the address list of the user, but not from the database

4. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

## Assigning a shared address to the user

### About this task

Use this procedure to choose a shared address for a user from the common addresses database. You can assign and remove a shared address.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, do one of the following:
  - To assign shared addresses to a new user while creating the user, click **New**.
  - To assign shared addresses to an existing user, select the user, and click **Edit**.
3. On the User Profile | Add page or the User Profile | Edit | <User Name> page, click **Identity > Address > Choose Shared Address**.
4. On the Choose Shared Address page, click one or more shared addresses.

For a new user, enter valid information in all mandatory fields on all tabs of the User Profile | Add page before you click **Commit**. If you enter invalid information, the system displays an error message.

5. Click **Select**.
6. Click one of the following:
  - **Commit**: To save the changes.
  - **Commit & Continue**: To save the changes and stay on the same page for making further modifications.

#### Related links

[Choose Address field descriptions](#) on page 257

### Add Address field descriptions

| Name                     | Description                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Address Name</b>      | The unique label that identifies the mailing address.                                                                            |
| <b>Address Type</b>      | The mailing address type such as home or office address.                                                                         |
| <b>Building</b>          | The name of the building.                                                                                                        |
| <b>Room</b>              | The number or name of the room.                                                                                                  |
| <b>Street</b>            | The name of the street.                                                                                                          |
| <b>City</b>              | The name of the city or town.                                                                                                    |
| <b>State or Province</b> | The full name of the province.                                                                                                   |
| <b>Postal Code</b>       | The postal code or zip code used by postal services to route mail to a destination. For the United States, specify the Zip code. |
| <b>Country</b>           | The name of the country.                                                                                                         |

#### Phone Details section

| Name                        | Description                                                                    |
|-----------------------------|--------------------------------------------------------------------------------|
| <b>Business Phone</b>       | The business phone number of the user.                                         |
| <b>Other Business Phone</b> | The secondary or alternate business phone number if applicable.                |
| <b>Home Phone</b>           | The residential phone number of the user.                                      |
| <b>Other Home Phone</b>     | The secondary or alternate residential phone number if applicable.             |
| <b>Mobile Phone</b>         | The mobile number of the user.                                                 |
| <b>Other Mobile Phone</b>   | The secondary or alternate mobile number of the user if applicable.            |
| <b>Fax</b>                  | The telephone number for direct reception of faxes.                            |
| <b>Pager</b>                | The number used to make calls to the pager of the user.                        |
| <b>Other Pager</b>          | The secondary or alternate number used to make calls to the pager of the user. |

| Button | Description                           |
|--------|---------------------------------------|
| Add    | Adds the mailing address of the user. |
| Cancel | Cancels the add address operation.    |

### Related links

[Modifying a shared address](#) on page 605

[Adding a shared address](#) on page 605

## Choose Address field descriptions

| Name         | Description                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------|
| Name         | The unique label that identifies the address.                                                                   |
| Address Type | The mailing address type such as home or office address.                                                        |
| Street       | The name of the street.                                                                                         |
| City         | The name of the city or town.                                                                                   |
| Postal Code  | The postal code used by postal services to route mail to a destination. In the United States, this is Zip code. |
| Province     | The full name of the province.                                                                                  |
| Country      | The name of the country.                                                                                        |

| Button | Description                                                                   |
|--------|-------------------------------------------------------------------------------|
| Select | Adds the selected mailing address as the shared contact for the user account. |
| Cancel | Cancels the choose address operation.                                         |

---

## Managing communication profiles

### Communication profiles

You can provide communication profiles to associate elements with users. Communication profiles support communication interactions established through Avaya Communication Services.

Communication profiles can be associated to the following entities:

- CM Endpoint
- Messaging
- Avaya Messaging
- Session Manager
- CS 1000
- IP Office
- Presence

- Avaya Breeze® platform
- Conferencing
- Avaya Meetings Server

You can provide communication profiles in User Management through Communication Profile Extension Pack (EP). You can use a communication profile to represent a subscription of the user to a communication subsystem and the specific configuration needs of the user. A communication subsystem is a service or infrastructure that manages the establishment and controls or routes the communication interactions.

System Manager supports maximum five communication profile sets for each user. You can add maximum three CM Endpoint profiles and one Messaging profile for each user, and the remaining two communication profile sets can contain other profiles.

## Adding a communication profile for the user

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, do one of the following:
  - To create a new user account, click **New**.
  - To add a communication profile to an existing user, select the user and click **Edit**.
3. On the User Profile | Add or the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the communication profile section, click **New**.
5. In the **Name** field, enter the name of the new communication profile.
6. **(Optional)** To mark the profile as default, select the **Default** check box.
7. Click **Done**.
8. Click **Commit**.

### Related links

[User Profile | Add field descriptions](#) on page 295

## Deleting the communication profile of a user

### About this task

You cannot delete default communication profiles.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, select a profile.

5. Click **Delete**.
6. Click **Commit**.

### Result

When you delete a communication profile, System Manager deletes all associated communication addresses.

## Creating a new communication address for a communication profile

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, do one of the following :
  - To create a new user account, click **New**.
  - To add a communication profile address to an existing user, select the user and click **Edit**.
3. On the User Profile | Add or User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, select a communication profile.
5. In the **Communication Address** section, click **New**.
6. In the **Type** field, enter a communication protocol.
7. In the **Fully Qualified Address** field, enter a contact address in the format supported by the value that you selected in the **Type** field. A contact address can be an e-mail ID, an instant messenger ID, or the SIP address of a SIP-enabled device.
8. Enter the domain name in the field next to **Fully Qualified Address** field.
9. Click **OK**.
10. Click **Commit**.

### Related links

[User Profile | Edit | <User Name> field descriptions](#) on page 315

[User Profile | Add field descriptions](#) on page 295

## Modifying the communication address

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, select a profile.
5. In the **Communication Address** section, select a communication address.
6. Click **Edit**.

7. Modify the information in the respective fields.
8. Click **OK**.
9. Click **Commit**.

#### Related links

[User Profile | Edit | <User Name> field descriptions](#) on page 315

[User Profile | Add field descriptions](#) on page 295

## Deleting a communication address from a communication profile

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **Communication Profile** section, click a communication profile.
5. In the **Communication Address** section, select a communication address from the table.
6. Click **Delete**.
7. Click **Commit**.

#### Related links

[User Profile | Edit | <User Name> field descriptions](#) on page 315

[User Profile | Add field descriptions](#) on page 295

## Session Manager communication profile administration

In the Session Manager Communication Profile section, you can associate a primary Session Manager instance as a home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura<sup>®</sup> network.

All communication addresses of type SIP for the communication profile are associated with the Avaya Aura<sup>®</sup> network. If you select a secondary Session Manager instance, Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager is unavailable.

You can configure the system to invoke application sequences when routing calls from (origination application sequence) or to (termination application sequence) the currently displayed user.

You can specify a conference factory set for users for improved voice, video and text conferencing.

For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile that is used when local connectivity to Session Manager instances in the Aura core is lost. If you select a Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues locally to the Communication Manager remote survivable server resident with the Branch Session Manager.

When this user calls numbers that are not associated with an administered user, the system applies dial-plan rules to complete the call based on this home location if the IP address of the SIP device used to make the call is unassigned to a location.

### Related links

[Multi Device Access](#) on page 261

[User Profile | Add field descriptions](#) on page 295

## Multi Device Access

With the Multi Device Access feature, a SIP user can register multiple SIP endpoints with the same extension. You can specify the maximum number of SIP endpoints that can simultaneously register and receive calls in the **Max. Simultaneous Devices** field of the Session Manager communication profile section on the User Profile page. The default is 1. For more information, see *Avaya Aura® Multi Device Access White Paper* on the Avaya Support site at <http://support.avaya.com/>.

If the number of registration requests exceed the administered limit, and if the **Block New Registration When Maximum Registrations Active** field is:

- Cleared, the system accepts the new registration and unregisters the endpoint with the oldest registration. If the endpoint with the oldest registration is active on a call, the system waits for the call to complete before unregistering.
- Selected, the system denies any new registrations and sends the 403 Forbidden response with an appropriate warning header to the registering device.

The system routes incoming INVITE requests or call attempts to all the registered devices for a given user simultaneously. When the caller answers the call, the system cancels the INVITE request to the other devices.

The system routes an incoming CANCEL request to all the registered devices if the caller hangs up before the call is answered.

## Lync integration simplification

In releases earlier than 7.0, for Lync integration, the administrator had to administer the Presence Services handle of an Avaya Aura® user twice as:

1. Avaya Presence/IM (formerly XMPP) handle
2. Avaya SIP handle

The duplicate administration was required for proper routing of the Lync originated subscription and IM requests.

Starting with Session Manager Release 7.0, the Presence Services handle is administered only once.

To support tighter integration with Microsoft Lync, Session Manager:

- Supports routing rules, configured in System Manager, to deliver Lync Presence/IM traffic to Presence and Avaya Multimedia Messaging as appropriate.
- Recognizes and routes on the Presence/IM handle type.

- Inserts the media type (mtype) parameter in the Route header when routing to SIP entities.

 **Note:**

The Lync server does not connect with a Branch Session Manager in branch locations.

## Presence communication profile administration

You can configure attributes for the Presence communication profile when you create a user or edit the existing user. You can also configure the Presence-related attributes by using the user provisioning rule.

In System Manager, you must configure the Avaya Aura® users and assign typically some or all of the following attributes:

- Avaya E.164 communication address
- Avaya SIP communication address
- CM Endpoint profile
- Session Manager profile

You can configure the attributes from **User Management > Manage Users**.

You can create Presence profiles only for the default communication profile.

 **Note:**

To create the Presence communication profile, you must select **Avaya Presence/IM** and provide the communication address.

## CM Endpoint profile administration

### CM Endpoint profile of a user

With User Profile Management, you can create the CM Endpoint communication profile for a user to create an association between an endpoint and a user.

You can add, view, modify, and delete endpoint profile. You can go to Endpoint Management pages to modify any of the endpoint fields that are not available through User Profile Management.

### Login name of endpoint profile

The login name in the Identity section on the User Profile | Add and User Profile | Edit | <User Name> pages is the user name that is associated with the CM Endpoint communication profile. This user name appears in the **User** column in the Endpoint List.

For endpoints, the **Localized Display Name** and **Endpoint Display Name** fields in the Identity section of the User Profile Management user profile map to the **Name** and **Localized Display Name** fields of CM Endpoint. The **Localized Display Name** and **Endpoint Display Name** fields are optional. They default to the **Last Name** and **First Name** as given in the General section of the User Profile Management user profile. You can also fill in any other name of your choice.



 **Note:**

**Endpoint Display Name** and **Localized Display Name** are auto populated while user creation is based on **Last Name** and **First Name**. **Endpoint Display Name** and **Localized Display Name** values get automatically changed if any change is made to **Last Name** and **First Name** value from User Import, Web Console or Web Service operation for user update.

If the **Endpoint Display Name** and **Localized Display Name** are edited manually (not based on Last Name/First Name) during user creation or user edit operation, then these values will never get auto changed even if changes are made to user's **Last Name** and **First Name** from User Import, Web Console or Web Service operation for user update.

## Creating CM Endpoint profile

You can create one default or primary Communication Profile for a user. To this default profile, you can add one CM Endpoint profile. You can add a maximum of three CM Endpoint profile per user.

## Adding a CM Endpoint profile for a user

### Before you begin

Add Communication Manager by using Manage Elements or Discovery from **Inventory**.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, do one of the following:
  - To create a CM Endpoint profile for a new user profile, click **New**.
  - To create a CM Endpoint profile for an existing user, select the user and click **Edit**.
3. Click the **Communication Profile** tab.
4. In the PROFILES section, click the toggle button next to **CM Endpoint Profile**.

System Manager enables **CM Endpoint Profile** and displays the fields of the CM Endpoint profile.

5. Perform the following:
  - a. In the **System** field, select the Communication Manager system to add an endpoint.
  - b. In the **Profile Type** field, select **Endpoint**.
  - c. In the **Extension** field, type the extension number, and then click the **Editor** button next to the given extension number.
  - d. In the **Template** field, select the required template for the endpoint.
  - e. In the **Set Type** field, select the required set type for the endpoint.
6. **(Optional)** To delete the endpoint from the communication management device after removing the association between the endpoint and the user, select the **Delete on Unassign from User or on Delete User** check box.
7. Perform one of the following:
  - To save the changes, click **Commit**.

- To save the changes and stay on the same page, click **Commit & Continue**.

#### Related links

[User Profile | Add field descriptions](#) on page 295

### Viewing the station profile of a user

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **View**.
3. Click the **Communication Profile** tab.

### Modifying the CM Endpoint profile of a user

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the CM Endpoint Profile section, modify the relevant information in the fields.
5. Do one of the following:
  - To save the changes to the database, click **Commit**.
  - To cancel the action and return to the previous page, click **Cancel**.

#### Related links

[User Profile | Add field descriptions](#) on page 295

### Using the automatically generated call routes for SIP routing

#### About this task

Based on the primary or secondary Session Manager that you specified in **Session Manager Communication Profile**, the system automatically determines a route pattern.

#### Before you begin

In the Communication Manager instance that you associated with System Manager, do the following:

1. On the Route Pattern page, specify the primary Session Manager.
2. Select a SIP endpoint.

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. Click **Communication Profile**.
3. In **Session Manager Profile > SIP Registration > Primary Session Manager**, click a primary Session Manager.

Ensure that you have added a primary Session Manager. To add a primary Session Manager, see *Administering Avaya Aura® Communication Manager*.

4. In **CM Endpoint Profile**, do the following:
  - a. In the **Set Type** field, enter the details of a SIP set type.
  - b. Select the **Calculate Route Pattern** check box.

### Result

The system automatically generates route patterns for the user that you specified and for the Session Manager that you set as the primary Session Manager.

## Removing association between an CM Endpoint and a user

### Before you begin

Ensure that you have not selected the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a station with a user.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and perform one of the following steps:
  - Click **Edit**.
  - Click **View > Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
5. Click **Commit**.

### Result

The system removes the association between the endpoint and the user. The endpoint is still provisioned on the communication management device.

## Deleting a CM Endpoint profile of a user

### Before you begin

Select the **Delete Endpoint on Unassign of Endpoint from User or Delete User** check box while associating a endpoint to a user.

### About this task

The delete functionality removes the association between the endpoint and the user, and deletes the endpoint from the communication management device.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user, and click **Edit**.

3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the **CM Endpoint Profile** section, clear the check box next to the **CM Endpoint Profile** label.
5. Click **Commit**.

 **Note:**

You can delete only those endpoints that are associated with a user through User Management. You can delete nonuser associated endpoints through Endpoint management.

## Related links

[User Profile | Add field descriptions](#) on page 295

## Messaging profile administration

### Messaging profile of a user

With User Profile Management, you can create the Messaging communication profile for a user to create an association between a subscriber mailbox and a user.

You can add, view, modify, and delete messaging profile. You can go to Subscriber Management pages to modify any of the subscriber fields that are not available through User Profile Management.

### Login name of messaging profile

The login name in the Identity section on the User Profile | Add and User Profile | Edit | <User Name> pages is the user name that is associated with the Messaging communication profile. This user name appears in the **User** column in the Subscriber List.

For Subscribers, the **Last Name** and **First Name** fields in the General section of User Profile Management user profile directly map to the **Last Name** and **First Name** fields in Subscriber. The **Localized Display Name** and **Endpoint Display Name** fields are not applicable for Subscribers.

### Creating Messaging profile

You can create one default or primary Communication Profile for a user. To this default profile, you can add one Messaging profile per user.

### Adding a messaging profile for a user

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, perform one of the following steps:
  - If you are creating a messaging profile for a new user profile, click **New**.
  - If you are creating a messaging profile for an existing user, select the user and click **Edit**.
3. Click the **Communication Profile** tab.
4. In the Messaging Profile section, select the check box next to the **Messaging Profile** label.

5. In the Messaging Profile section, complete the relevant fields.

 **Note:**

To delete the subscriber mailbox from the communication management device after removing the association between the subscriber and the user, select the **Delete Messaging on Unassign of Subscriber from User or Delete User** check box.

6. Click **Commit** or **Commit & Continue** to add the messaging profile, or click **Cancel** to return to the previous page.

The field names that are marked with an asterisk (\*) are mandatory fields. You must enter valid information in these fields to create the CM Endpoint profile.

 **Note:**

You must add the messaging devices through Runtime Topology System (RTS) before you add a messaging profile for a user. After you create the user-subscriber association, the user name appears in the **User** column in the subscriber list.

## Related links

[User Profile | Add field descriptions](#) on page 295

## Modifying a messaging profile of a user

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the PROFILES section, click Messaging Profile, and modify the relevant information in the fields.
5. Perform one of the following:
  - To save the changes to the database, click **Commit**.
  - To save the changes to the database and remain on the same page, click **Commit & Continue**.
  - To cancel the action and return to the previous page, click **Cancel**.

## Related links

[User Profile | Add field descriptions](#) on page 295

## Viewing a messaging profile of a user

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **View**.
3. Click the **Communication Profile** tab.

## Result

The Messaging Profile section displays the messaging profile information of the user.

## Related links

[User Profile | Add field descriptions](#) on page 295

## Removing association between a subscriber mailbox and a user

### Before you begin

The **Delete Subscriber on Unassign of Subscriber from User or Delete User** check box is clear while associating a mailbox with a user.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the Messaging Profile tab, clear the check box next to the **Messaging Profile** label.
5. Click **Commit**.

## Result

The system removes the association between the subscriber mailbox and the user. The subscriber mailbox is still provisioned on the communication management device.

## Deleting a subscriber mailbox

### Before you begin

You have selected the **Delete Subscriber on Unassign of Subscriber from User or on Delete User** check box while associating a subscriber mailbox to a user.

### About this task

This functionality deletes the subscriber mailbox from the messaging device after removing the association between the subscriber mailbox and the user.

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the Messaging Profile section, clear the check box next to the **Messaging Profile** label.
5. Click **Commit**.

### **Note:**

You can delete only those subscribers that are associated with a user through User Management. You can delete non-user associated subscriber mailboxes only through Subscriber Management.

## CS 1000 profile administration

### CS 1000 profile administration

With User Management, you can create CS 1000 Endpoint Profile to create an association between an endpoint and a user.

To modify an endpoint or subscriber field that is not available through User Management, navigate to the Endpoint or Subscriber Management pages and modify the information. For information, see [Redirecting the CS 1000 user to Element Manager](#).

### Related links

[Redirecting the CS 1000 user to Element Manager](#) on page 269

### Redirecting the CS 1000 user to Element Manager

#### Before you begin

A user must exist with at least one communication profile.

To create a new user, navigate to **Users > User Management > Manage Users > New**.

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
4. In the PROFILES section, click **CS 1000 Endpoint Profile** that you must update and click **Update**.

The system displays the user profile in the element manager that you select.

#### **Note:**

The system discards all unsaved changes that you make to the current user including the changes to communication profiles.

5. Enter the relevant information and click **Save**.

The system displays the Manage Users page.

### Adding a CS 1000 profile for a user

#### Before you begin

A user must exist.

To create a new user, navigate to **Users > User Management > Manage Users > New**.

#### About this task

For a communication profile, you can provide a maximum of one CS 1000 phone. To add additional phones for a user, you must add another communication profile.

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.

2. On the Manage User page, perform one of the following steps:
    - To create a profile for a new user profile, click **New**.
    - To create a profile for an existing user, select the user and click **Edit**.
  3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.
  4. In the **CS1000 Endpoint Profile** section, select the check box and complete the following fields:
    - a. In the **System** field, select a CS 1000 system.

The system displays a list of systems that are registered with the element registry.
    - b. Perform one of the following:
      - Click **Add new** and complete the following fields:
        - a. In the **Target** field, select a CS 1000 customer number.
        - b. In the **Template** field, select a template that CS 1000 Element Manager provides.
        - c. In the **Primary DN** field, enter a preferred primary DN.
    -  **Note:**

If you do not provide a primary DN, CS 1000 Element Manager automatically assigns a primary DN.
    - d. In the **Terminal Number** field, enter a preferred TN.
  - Click **Link existing**, and in the **Existing TN** field, enter the terminal number from the list of existing numbers.
  - c. Clear the **Include in Corporate Directory** check box to exclude the profile in the CS 1000 corporate directory.
  - d. **(Optional)** Select **Delete Endpoint on Unassign of Endpoint from User** if you must delete the endpoint from CS 1000 when you remove the association between the endpoint and the user.
5. Perform one of the following:
  - To save the changes to the database, click **Commit**.
  - To save the changes to the database and remain on the same page, click **Commit & Continue**.
  - To cancel the action and return to the previous page, click **Cancel**.

## Modifying a CS 1000 user profile

### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, select a user and click **Edit**.
3. On the User Profile | Edit | <User Name> page, click the **Communication Profile** tab.



4. Click **Update**.
5. In the CS 1000 Element Manager window, enter the relevant information in the fields.

 **Note:**

In CS 1000 Element Manager, do not update the CPND name. The system maps the CPND name to the System Manager UPM user **Localized Display Name**. Use System Manager UPM to update the CPND name. For more details, see the “Communication profiles synchronization” section.

6. Perform one of the following:
  - To save the changes to the database, click **Commit**.
  - To save the changes to the database and remain on the same page, click **Commit & Continue**.
  - To cancel the action and return to the previous page, click **Cancel**.

## Changing passwords of CS 1000 Presence users

### Procedure

1. To log on to the System Manager personal agent console, enter `http://<SMGR server-name>/pa`.
2. Click **Change Password**.
3. Enter the old and new passwords, and then click **Save**.

Presence Services recognizes the password change.

 **Note:**

The system needs a synchronized password that is the same password as the password that Presence Services uses to update CS 1000.

## IP Office profile administration

### Adding an IP Office endpoint profile on a user

#### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
  - To create a profile for a new user, click **New**.
  - To create a profile for an existing user, select the user and click **Edit**.
4. On the User Profile page, click the **Communication Profile** tab.
5. Select the **IP Office Endpoint Profile** check box.
6. Complete the **IP Office Endpoint Profile** section.

7. Perform one of the following:

- To save the changes to the database, click **Commit**.
- To save the changes to the database and remain on the same page, click **Commit & Continue**.
- To cancel the action and return to the previous page, click **Cancel**.

 **Note:**

To assign an extension to the user, perform one of the following actions:

- Assign an available extension to the user, select the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.
- Or assign an available module-port to the user from the **Module-Port** drop-down box, and type the new extension. The module-port combination is valid only when you associate a digital or an analog extension type to the user.

To assign an extension to a user with other set types, perform one of the following actions:

- Type an appropriate extension.
- Select the **Use Existing Extension** check box to choose an existing extension.
- Select an unassigned extension from the drop-down field.

**Related links**

[User Profile | Add field descriptions](#) on page 295

**Viewing an IP Office endpoint profile of a user  
Procedure**

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select the user whose profile you want to view.
4. Click **View**.
5. Click the **Communication Profile** tab.

Click the **IP Office Endpoint** section to view the IP Office endpoint profile of the user you selected.

**Related links**

[User Profile | Add field descriptions](#) on page 295

**Modifying an IP Office endpoint profile of a user  
Procedure**

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.

3. On the User Management page, select the user whose profile you want to edit.
4. Click **Edit**.
5. Select the **Communication Profile** tab.
6. Edit the required fields in the **IP Office Endpoint Profile** section.
7. Perform one of the following:
  - To save the changes to the database, click **Commit**.
  - To save the changes to the database and remain on the same page, click **Commit & Continue**.
  - To cancel the action and return to the previous page, click **Cancel**.

 **Note:**

To assign an extension to the user, perform one of the following actions:

- Assign an available extension to the user, select the **Use Existing Extension** check box, and select an unassigned extension from the drop-down box.
- Or assign an available module-port to the user from the **Module-Port** drop-down box, and type the new extension. The module-port combination is valid only when you associate a digital or an analog extension type to the user.

To assign an extension to a user with other set types, perform one of the following actions:

- Type an appropriate extension.
- Select the **Use Existing Extension** check box to choose an existing extension.
- Select an unassigned extension from the drop-down field.

## Related links

[User Profile | Add field descriptions](#) on page 295

## Removing the association between an IP Office endpoint profile and a user

### About this task

You must add, edit, or delete the end point profile for a user with an IP Office Endpoint profile only when IP Office is active and connected to System Manager.

 **Note:**

Do not perform the add, edit, or delete operations when IP Office is temporarily unreachable. However, in situations when IP Office is unused or corrupted, you must set the `force_delete_user` property to true in the `IPOffice.properties` file by using putty to delete IP Office Endpoint Profile from System Manager users.

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.

3. On the User Management page, select a user, and perform one of the following:
  - Click **Edit**.
  - Click **View > Edit**.
4. On the User Profile Edit page, click the **Communication Profile** tab.
5. Clear the **IP Office Endpoint Profile** check box.
6. Click **Commit**.

#### Related links

[Removing the association between an IP Office endpoint profile and a user from the properties file](#) on page 274

#### *Removing the association between an IP Office endpoint profile and a user from the properties file*

##### About this task

Use the procedure to remove association between an IP Office endpoint profile and a user only when IP Office is unused or corrupted.

##### Procedure

1. Using putty, navigate to the `$ABG_Home/tools` folder.
2. Open the `IPOffice.properties` file, and set the `force_delete_user` property to true.  
By default, the `force_delete_user` property is set to false to ensure that the user data on IP Office and System Manager is synchronized.
3. Save the properties file.
4. To restart the JBoss service, at the prompt, type `service jboss restart`.  
Wait until the JBoss service starts.
5. On System Manager web console, click **Users > User Management** and delete the IP Office Endpoint Profile of the user that exist on the abandoned or corrupted IP Office.
6. Set the `force_delete_user` property to false and restart the JBoss service.

#### Related links

[Removing the association between an IP Office endpoint profile and a user](#) on page 273

---

## Managing default contact list of the user

### Adding a contact in the Default Contact list

#### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following:
  - To add a contact for a new user, click **New**.
  - To add a contact for an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.
5. In the **Default Contact List** section, enter a brief description of the contact list in the **Description** field.
6. In the **Associated Contacts** section, click **Add**.
7. On the Attach Contacts page, select one or more contacts and click **Select**.

 **Note:**

In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:

- Private contacts of the user
- Public contacts
- Users who belong to that tenant

The system displays the new contacts in the table in the **Associated Contacts** section.

#### Related links

[Attach Contacts field descriptions](#) on page 276

## Modifying membership details of a contact in a contact list

### About this task

Use this feature to set the speed dial and presence buddy information for the contacts in the Default Contact list.

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the **Associated Contacts** section, select a contact and click **Edit**.
6. On the Edit Contact List Member page, in the **Contact Membership Details** section, change the required information in the fields.

You can only change the information in the fields displayed in the **Contact Membership Details** section.

7. Click **Add**.
8. Click **Commit** to save the changes.

## Related links

[Edit Contact List Member field descriptions](#) on page 278

## Viewing membership details of a contact in the contact list

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. On the User Profile View page, click the **Contacts** tab.
5. In the Associated Contacts section, click the last name link under the **Last Name** column.

### Result

The View Contact List Member page displays the details of the selected contact.

## Related links

[View Contact List Member field descriptions](#) on page 279

## Deleting contacts from the default contact list

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. Select one or more contacts from the Associated Contacts section and click **Remove**.

## Attach Contacts field descriptions

In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:

- Private contacts of the user
- Public contacts
- Users who belong to that tenant

| Name               | Description                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------|
| Last Name          | The last name of the contact.                                                                         |
| First Name         | The first name of the contact.                                                                        |
| Scope              | The categorization of the contact based on whether the contact is a user, public, or private contact. |
| Display/Login Name | The unique login name or display name of the contact.                                                 |

*Table continues...*

| Name                   | Description                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Contact Address</b> | The address of a private or public contact. No contact address is associated with a contact type user.                |
| <b>User Handles</b>    | The communication handles associated with the user. These handles are defined in the communication profile of a user. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                        |
| <b>Filter: Enable</b>  | Displays fields under selected columns that you can use to set the filter criteria. This is a toggle button.          |
| <b>Filter: Apply</b>   | Filters contacts based on the filter criteria.                                                                        |
| <b>Advanced Search</b> | Displays fields that you can use to specify the search criteria to search for contacts.                               |

| Button        | Description                                                   |
|---------------|---------------------------------------------------------------|
| <b>Select</b> | Adds the selected contact in the list of associated contacts. |
| <b>Cancel</b> | Cancels your selection and takes you to the Contacts tab.     |

The page displays the following fields when you click **Advanced Search** at the upper-right corner of the contact table.

| Name             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Search On</b> | The search options that must base on the <b>Contact</b> or <b>User</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Criteria</b>  | <p>The search criteria for searching the contacts. Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Field 1 - The list of criteria that you can use to search the contacts. You can search based on the first name, last name, or the address/handle of the contact.</li> <li>• Field 2 - The operators for evaluating the expression. Based on the search criterion which you select in the first drop-down field, only those operators that are applicable for the selected criterion are displayed in the second drop-down field.</li> <li>• Field 3 - The value for the search criterion.</li> </ul> |

| Button   | Description                                                                                                |
|----------|------------------------------------------------------------------------------------------------------------|
| <b>+</b> | Adds one more search criteria section.                                                                     |
| <b>-</b> | Clears the last search criteria. This button is applicable only if there is more than one search criteria. |

## Edit Contact List Member field descriptions

### Contact Membership Details

| Field                    | Description                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Label</b>             | The text description for classifying this contact.                                                                                             |
| <b>Alternative Label</b> | The text description for classifying this contact. The field is similar to <b>Label</b> , and is used to store label in an alternate language. |
| <b>Description</b>       | The brief description about the contact.                                                                                                       |
| <b>Presence Buddy</b>    | An option to indicate whether to allow monitoring of the presence information of the contact.                                                  |
| <b>Speed Dial</b>        | An option to indicate whether to allow speed dial for the contact.                                                                             |
| <b>Address/Handle</b>    | The fully qualified URI for interacting with the contact. This field is available only if you select the <b>Speed Dial</b> check box.          |
| <b>Speed Dial Entry</b>  | The reduced number that represents the speed dial number. This field is available only if you select the <b>Speed Dial</b> check box.          |

### Contact Details

| Field                         | Description                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------|
| <b>Last Name</b>              | The last name of the contact.                                                                  |
| <b>First Name</b>             | The first name of the contact.                                                                 |
| <b>Middle Name</b>            | The middle name of the contact.                                                                |
| <b>Description</b>            | The brief description about the contact.                                                       |
| <b>Company</b>                | The name of the company to which the contact belongs.                                          |
| <b>Localized Display Name</b> | The localized display name of a user. The name is usually the localized full name.             |
| <b>Endpoint Display Name</b>  | The endpoint display name of the contact.                                                      |
| <b>Language Preference</b>    | The list of languages from which you set a language as the preferred language for the contact. |
| <b>Update Time</b>            | The time when the contact information was last updated.                                        |
| <b>Source</b>                 | The source of provisioning the contact.                                                        |

### Postal Address

| Field                | Description                                                  |
|----------------------|--------------------------------------------------------------|
| <b>Name</b>          | The name of the contact.                                     |
| <b>Address Type</b>  | The type of mailing address such as, home or office address. |
| <b>Street</b>        | The name of the street.                                      |
| <b>Locality Name</b> | The name of the city or town.                                |
| <b>Postal Code</b>   | The postal code of the locality of the city or town.         |

*Table continues...*



| Field           | Description                                   |
|-----------------|-----------------------------------------------|
| <b>Province</b> | The full name of the province of the contact. |
| <b>Country</b>  | The name of the country of the contact.       |

### Contact Address

| Field                    | Description                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | The address that you can use to communicate with the contact. The address can be a phone number, email address, or IM of the contact.     |
| <b>Type</b>              | The type of communication medium for interacting with the user.                                                                           |
| <b>Category</b>          | The categorization of the address based on the location.                                                                                  |
| <b>Label</b>             | The description for classifying this contact.                                                                                             |
| <b>Alternative Label</b> | The description for classifying this contact. The field is similar to <b>Label</b> , and is used to store label in an alternate language. |

| Button     | Description                                     |
|------------|-------------------------------------------------|
| <b>Add</b> | Saves the modified information in the database. |

## View Contact List Member field descriptions

### Contact Membership Details

| Name                     | Description                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                                                                |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. The <b>Alternative Label</b> field is similar to <b>Label</b> , but you use the field to store label in an alternate language. |
| <b>Description</b>       | Displays a brief description about the contact.                                                                                                                                          |
| <b>Presence Buddy</b>    | Provides the option to indicate whether to allow monitoring of the presence information of the contact.                                                                                  |
| <b>Speed Dial</b>        | Provides the option to indicate whether to allow speed dial for the contact.                                                                                                             |
| <b>Address/Handle</b>    | Displays a fully qualified URI for interacting with the contact. This field is available only if you select the <b>Speed Dial</b> check box.                                             |
| <b>Speed Dial Entry</b>  | Displays the reduced number that represents the speed dial number. This field is available only if you select the <b>Speed Dial</b> check box.                                           |

### Contact Details

| Name               | Description                              |
|--------------------|------------------------------------------|
| <b>Last Name</b>   | Displays the last name of the contact.   |
| <b>First Name</b>  | Displays the first name of the contact.  |
| <b>Middle Name</b> | Displays the middle name of the contact. |

*Table continues...*

| Name                          | Description                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Description</b>            | Displays a brief description about the contact.                                                         |
| <b>Company</b>                | Displays the name of contact's company                                                                  |
| <b>Localized Display Name</b> | Displays the localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Displays the endpoint display name of the contact.                                                      |
| <b>Language Preference</b>    | Displays a list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | Displays the time when the contact information was last updated.                                        |
| <b>Source</b>                 | Displays the source of provisioning the contact.                                                        |

## Postal Address

| Name                | Description                                                        |
|---------------------|--------------------------------------------------------------------|
| <b>Name</b>         | Displays the name of the contact.                                  |
| <b>Address Type</b> | Displays the mailing address type such as, home or office address. |
| <b>Street</b>       | Displays the name of the street.                                   |
| <b>City</b>         | Displays the name of the city or town.                             |
| <b>Postal Code</b>  | Displays the postal code of the locality of the city or town.      |
| <b>Province</b>     | Displays the full name of the contact's province.                  |
| <b>Country</b>      | Displays the name of the contact's country.                        |

## Contact Address

| Name                     | Description                                                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | Displays the address that you can use to communicate with the contact. This can be a phone number, email address, or IM of the contact.                   |
| <b>Type</b>              | Displays the type of communication medium for interacting with the user.                                                                                  |
| <b>Category</b>          | Displays the categorization of the address based on the location.                                                                                         |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                                 |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This field is similar to <b>Label</b> , but it is used to store label in an alternate language. |

---

## Managing private contacts of a user

### Adding a private contact to a user

#### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following steps:
  - To add a private contact while setting up a new user, click **New**.
  - To add a private contact to an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, click **New**.
6. On the New Private Contact page, enter the last name, first name, middle name, description, company name, localized display name, endpoint display name, and language preference in the Contact Details section.  
Enter a valid information in the fields.
7. In the Postal Address section, click **New** to choose a postal address for the contact.  
You can click **Choose Shared Address** to choose a shared address for a contact.
8. In the Contact Address section, click **New** to choose a contact address for the contact.
9. Click **Add** to add the private contact.
10. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

#### Related links

[New Private Contact field descriptions](#) on page 286

## Modifying details of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the **Private Contacts** area, select a contact.
6. Click **Edit**.
7. On the Edit Private Contact page, modify the information of the contact.
8. Click **Add** to save the modified information.

#### Related links

[Edit Private Contact field descriptions](#) on page 288

## Viewing details of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.

2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **View**.
4. On the User Profile View page, click the **Contacts** tab.
5. Click **Private Contacts**.
6. In the Private Contacts section, click the link displayed in the **Last Name** column for a contact.

The View Private Contact page displays the details of the contact whose last name you have clicked.

#### Related links

[View Private Contact field descriptions](#) on page 289

## Deleting private contacts of a user

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select one or more contacts from the table displaying private contacts.
6. Click **Delete**.
7. On the **Contact Delete Confirmation** page, click **Delete**.

The system displays the User Profile Edit page.

8. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

## Adding a postal address of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
  - If you are adding a postal address of a private contact to a new user, click **New**.
  - If you are adding a postal address of a private contact to an existing user, select a user and click **Edit**.
4. Click the **Contacts** tab.

5. In the **Private Contacts** area, perform one of the following:
  - If you are adding a postal address for a new private contact, click **New**.
  - If you are adding a postal address for an existing private contact, select a private contact and click **Edit**.
6. On the New Private Contact or Edit Private Contact page, click **New** in the Postal Address section.
7. On the Add Address page, enter the required information in the respective fields.  
Enter valid information in these fields.
8. Click **Add** to create a new postal address for the private contact.

#### Related links

[Add Address field descriptions](#) on page 256

## Modifying postal address of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select an address from the **Postal Address** area.
7. Click **Edit**.
8. On the Edit Address page, modify the information in the respective fields.  
Enter valid information in the fields.
9. Click **Add**.
10. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

#### Related links

[Edit Address field descriptions](#) on page 291

## Deleting postal addresses of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.

4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select one or more addresses from the **Postal Address** area.
7. Click **Delete**.
8. Click **Add**.

## Choosing a shared address for a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, perform one of the following steps:
  - To choose a shared address for a private contact while creating a new user, click **New**.
  - To choose a shared address for a private contact of an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, perform one of the following actions:
  - To add a new contact and add an address to the contact, click **New**.
  - To add an address to an existing contact, select the contact and click **Edit**.
6. On the New Private Contact or the Edit Private Contact page, click **Choose Shared Address** in the **Postal Address** area.
7. On the Choose Address page, select one or more shared addresses.
8. Click **Select**.
9. Click **Add** to add the selected addresses to the private contact.
10. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

### Related links

[Choose Address field descriptions](#) on page 257

## Adding a contact address for a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.

3. On the User Management page, perform one of the following steps:
  - To add a contact address of a private contact while creating a new user, click **New**.
  - To add a contact address of a private contact for an existing user, select the user and click **Edit**.
4. Click the **Contacts** tab.
5. In the Private Contacts section, perform one of the following steps:
  - To add a contact address for a new private contact, click **New**.
  - To add a contact address for an existing private contact, select the private contact from the list and click **Edit**.
6. On the New Private Contact or the Edit Private Contact page, click **New** in the **Contact Address** area.
7. On the Add Address page, enter the appropriate information in the respective fields.  
Enter a valid information in these fields.
8. Click **Add**.
9. Perform one of the following:
  - To save the changes, click **Commit**.
  - To save the changes and stay on the same page, click **Commit & Continue**.

#### Related links

[Add Address field descriptions](#) on page 290

## Modifying a contact address of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contacts section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select a contact address from the **Contact Address** area.
7. Click **Edit**.
8. On the Edit Address page, modify the information in the respective fields.  
Enter valid information in these fields.
9. Click **Add** to save the modified address.
10. On the Edit Private Contact page, click **Add**.  
The system displays the User Profile Edit page.

11. Perform one of the following:

- To save the changes, click **Commit**.
- To save the changes and stay on the same page, click **Commit & Continue**.

#### Related links

[Edit Address field descriptions](#) on page 291

## Deleting contact addresses of a private contact

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, select a user and click **Edit**.
4. On the User Profile Edit page, click the **Contacts** tab.
5. In the Private Contact section, select a contact and click **Edit**.
6. On the Edit Private Contact page, select one or more addresses from the Contact Address section.
7. Click **Delete**.
8. Click **Commit**.

## New Private Contact field descriptions

### Contact Details

| Name                   | Description                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------|
| Last Name              | The last name of the contact.                                                                    |
| First Name             | The first name of the contact.                                                                   |
| Middle Name            | The middle name of the contact.                                                                  |
| Description            | A brief description about the contact.                                                           |
| Company                | The name of contact's company.                                                                   |
| Localized Display Name | The localized display name of a user. It is typically the localized full name.                   |
| Endpoint Display Name  | The endpoint display name of the contact.                                                        |
| Language Preference    | The list of languages from which you set one language as the preferred language for the contact. |

### Postal Address

| Name         | Description                                               |
|--------------|-----------------------------------------------------------|
| Address Name | The unique label that identifies the address.             |
| Address Type | The mailing address type such as, home or office address. |

*Table continues...*



| Name                     | Description                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------|
| <b>Building</b>          | The name of the building.                                                                 |
| <b>Room</b>              | The name or number of the room.                                                           |
| <b>Street</b>            | The name of the street.                                                                   |
| <b>City</b>              | The name of the city or town of the contact.                                              |
| <b>State or Province</b> | The full name of the state or province where the contact's office or home is located.     |
| <b>Postal Code</b>       | The postal code of the of the city or town where the contact's office or home is located. |
| <b>Country</b>           | The name of the country where the contact's office or home is located.                    |

| Button                       | Description                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>                  | Displays the <b>Edit Address</b> page where you can modify an existing postal address of the private contact. |
| <b>New</b>                   | Displays the <b>Add Address</b> page where you can add a new postal address of the private contact.           |
| <b>Delete</b>                | Deletes the selected postal address.                                                                          |
| <b>Choose Shared Address</b> | Displays the <b>Choose Address</b> page where you can choose addresses of the private contact.                |

## Contact Address

| Name                     | Description                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | The address that you can use to communicate with the contact. This can be a phone number, email address, or IM of the contact.                   |
| <b>Type</b>              | The type of communication medium for interacting with the user.                                                                                  |
| <b>Category</b>          | The categorization of the address based on the location.                                                                                         |
| <b>Label</b>             | A text description for classifying this contact.                                                                                                 |
| <b>Alternative Label</b> | A text description for classifying this contact. This field is similar to <b>Label</b> , but it is used to store label in an alternate language. |

| Button        | Description                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------|
| <b>Edit</b>   | Displays the <b>Edit Address</b> page. Use this page to edit a contact address of the private contact. |
| <b>New</b>    | Displays the <b>Add Address</b> page. Use this page to add a contact address of the private contact.   |
| <b>Delete</b> | Deletes the selected contact address.                                                                  |

| Button     | Description                                                                                                                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add</b> | Creates a new contact.<br><br> <b>Note:</b><br>Enter valid information in the mandatory fields to successfully create a new contact. |

## Edit Private Contact field descriptions

### Contact Details

| Name                          | Description                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>              | Displays the last name of the contact.                                                                  |
| <b>First Name</b>             | Displays the first name of the contact.                                                                 |
| <b>Middle Name</b>            | Displays the middle name of the contact.                                                                |
| <b>Description</b>            | Displays a brief description about the contact.                                                         |
| <b>Company</b>                | Displays the name of contact's company                                                                  |
| <b>Localized Display Name</b> | Displays the localized display name of a user. It is typically the localized full name.                 |
| <b>Endpoint Display Name</b>  | Displays the endpoint display name of the contact.                                                      |
| <b>Language Preference</b>    | Displays a list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>            | Displays the time when the contact information was last updated.                                        |
| <b>Source</b>                 | Displays the source of provisioning the contact.                                                        |

### Postal Address

| Name                | Description                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------|
| <b>Name</b>         | Displays the unique label that identifies the address.                                             |
| <b>Address Type</b> | Displays the mailing address type such as, home or office address.                                 |
| <b>Street</b>       | Displays the name of the street.                                                                   |
| <b>City</b>         | Displays the name of the city or town.                                                             |
| <b>Postal Code</b>  | Displays the postal code of the of the city or town where the contact's office or home is located. |
| <b>Province</b>     | Displays the full name of the province where the contact's office or home is located.              |
| <b>Country</b>      | Displays the name of the country where the contact's office or home is located.                    |

| Button      | Description                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the <b>Edit Address</b> page. Use this page to modify an existing postal address of the private contact. |

*Table continues...*

| Button                       | Description                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>New</b>                   | Displays the <b>Add Address</b> page. Use this page to add new postal address of the private contact. |
| <b>Delete</b>                | Deletes the selected contact address.                                                                 |
| <b>Choose Shared Address</b> | Displays the <b>Choose Address</b> page. Use this page to choose addresses of the private contact.    |

## Contact Address

| Name                     | Description                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.              |
| <b>Type</b>              | Displays the type of communication medium for interacting with the user.                                                                              |
| <b>Category</b>          | Displays the categorization of the address based on the location.                                                                                     |
| <b>Label</b>             | Displays the text description for classifying this contact.                                                                                           |
| <b>Alternative Label</b> | Displays the text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language. |

| Button        | Description                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------|
| <b>Edit</b>   | Displays the <b>Edit Address</b> page. Use this page to edit a contact address of the private contact. |
| <b>New</b>    | Displays the <b>Add Address</b> page. Use this page to add a contact address of the private contact.   |
| <b>Delete</b> | Deletes the selected private contacts.                                                                 |

| Button     | Description                                     |
|------------|-------------------------------------------------|
| <b>Add</b> | Saves the modified information to the database. |

## View Private Contact field descriptions

### Contact Details

| Name                          | Description                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------|
| <b>Last Name</b>              | Displays the last name of the contact.                                                  |
| <b>First Name</b>             | Displays the first name of the contact.                                                 |
| <b>Middle Name</b>            | Displays the middle name of the contact.                                                |
| <b>Description</b>            | Displays a brief description about the contact.                                         |
| <b>Company</b>                | Displays the name of contact's company                                                  |
| <b>Localized Display Name</b> | Displays the localized display name of a user. It is typically the localized full name. |
| <b>Endpoint Display Name</b>  | Displays the endpoint display name of the contact.                                      |

*Table continues...*

| Name                       | Description                                                                                             |
|----------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Language Preference</b> | Displays a list of languages from which you set one language as the preferred language for the contact. |
| <b>Update Time</b>         | Displays the time when the contact information was last updated.                                        |
| <b>Source</b>              | Displays the source of provisioning the contact.                                                        |

### Postal Address

| Name                | Description                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------|
| <b>Name</b>         | Displays the unique label that identifies the address.                                             |
| <b>Address Type</b> | Displays the mailing address type such as, home or office address.                                 |
| <b>Street</b>       | Displays the name of the street.                                                                   |
| <b>City</b>         | Displays the name of the city or town.                                                             |
| <b>Postal Code</b>  | Displays the postal code of the of the city or town where the contact's office or home is located. |
| <b>Province</b>     | Displays the full name of the contact's province.                                                  |
| <b>Country</b>      | Displays the name of the contact's country.                                                        |

### Contact Address

| Name                     | Description                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.            |
| <b>Type</b>              | Displays the type of communication medium used to interact with the user.                                                                           |
| <b>Category</b>          | Displays the categorization of the address based on the location.                                                                                   |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                           |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language. |

| Button      | Description                       |
|-------------|-----------------------------------|
| <b>Done</b> | Returns you to the previous page. |

## Add Address field descriptions

Use this page to add communication address of the contact.

| Name           | Description                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b> | Displays the address that you can use to communicate with the contact. This can be a phone number, e-mail address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the <b>Type</b> field. |

*Table continues...*

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>              | Displays the type of address. The types of addresses are: <ul style="list-style-type: none"> <li>• <b>Phone</b>: This address type supports phone numbers.</li> <li>• <b>SIP</b>: This address type supports SIP-based communication.</li> <li>• <b>MSRTC</b>: This address type supports communication with a Microsoft RTC server.</li> <li>• <b>IBM Sametime</b>: This address type supports communication with IBM Sametime. Specify the address in the DN=IBMHandle format.</li> <li>• <b>XMPP</b>: This address type supports xmpp-based communication.</li> <li>• <b>SMTP</b>: This address type supports communication with the SMTP server.</li> </ul> |
| <b>Category</b>          | Displays the categorization of the address based on the location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Button     | Description                                                     |
|------------|-----------------------------------------------------------------|
| <b>Add</b> | Adds the contact address of the public contact to the database. |

### Related links

[Adding a contact address of a public contact](#) on page 596

## Edit Address field descriptions

Use this page to edit the details of a contact's communication address.

| Name           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b> | Displays the address that you can use to communicate with the contact. This can be a phone number, email address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the <b>Type</b> field.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Type</b>    | Displays the type of address. The types of addresses are: <ul style="list-style-type: none"> <li>• <b>Phone</b>: This address type supports phone numbers.</li> <li>• <b>SIP</b>: This address type supports SIP-based communication.</li> <li>• <b>MSRTC</b>: This address type supports communication with a Microsoft RTC server.</li> <li>• <b>IBM Sametime</b>: This address type supports communication with IBM Sametime. Specify the address in the DN=IBMHandle format.</li> <li>• <b>XMPP</b>: This address type supports xmpp-based communication.</li> <li>• <b>SMTP</b>: This address type supports communication with the SMTP server.</li> </ul> |

*Table continues...*

| Name                     | Description                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Category</b>          | Displays the categorization of the address based on the location.                                                                                   |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                           |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language. |

| Button     | Description                                     |
|------------|-------------------------------------------------|
| <b>Add</b> | Saves the modified information to the database. |

### Related links

[Modifying the details of a public contact](#) on page 597

## User Management field descriptions

### Tenant organization

The page displays the tenant organization that the administrator configured on the **Services > Tenant Management** page.

 **Note:**

The system displays the tenant-related section only when the Multi Tenancy feature is enabled on this system.

| Name                                                                                                     | Description                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b>                                                                                  | Select the check box for the tenant from the list of tenants to view the organization hierarchy.<br>Select the check box at each level to view the hierarchy. |
| <b>Enable auto refresh</b>                                                                               | Updates the information in the <b>Users</b> section automatically based on the selection in the tenant organization hierarchy.                                |
|  <b>Refresh Users</b> | Updates the tenant organization hierarchy.<br>Use this to view the changes that the administrator makes from <b>Services &gt; Tenant Management</b> .         |
| <b>Search</b>                                                                                            | Searches and displays the tenant organization.                                                                                                                |
| <b>Clear</b>                                                                                             | Clears the search criteria.                                                                                                                                   |

### Users

| Name                | Description                                          |
|---------------------|------------------------------------------------------|
| <b>Last Name</b>    | The last name of the user.                           |
| <b>First Name</b>   | The first name of the user.                          |
| <b>Display Name</b> | The unique name of the user displayed by the system. |
| <b>Login Name</b>   | The unique name that gives access to the system.     |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP Handle</b>             | The unique communication address of the user.                                                                                                                                                                                                                                                                                                            |
| <b>Organization Hierarchy</b> | <p>The hierarchy of the tenant organization in the format Tenant/Site/Department/Team.</p> <p>For example, Citi/Pune/HomeLoans/LoanSupport</p> <p> <b>Note:</b></p> <p>The system displays the field only when the administrator enables the Multi Tenancy feature.</p> |
| <b>Last Login</b>             | The date and time when the user successfully logged into the system.                                                                                                                                                                                                                                                                                     |

| Icon                                                                              | Description                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Searches for users on the basis of first name, last name, login name, surname, handles, first name (Latin translation) and last name (Latin translation).</p> <p>You can view, edit, or delete a user in the list.</p> |

| Button                                                  | Description                                                                                                |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>View</b>                                             | Displays the User Profile   View   <User Name> page where you can view the details of the selected user.   |
| <b>Edit</b>                                             | Displays the User Profile   Edit   <User Name> page where you can modify the details of the selected user. |
| <b>New</b>                                              | Displays the User Profile   Add page where you can create a new user.                                      |
| <b>Duplicate</b>                                        | Displays the User Profile   Duplicate   <User Name> page where you can create a duplicate user.            |
| <b>Delete</b>                                           | Displays the User Delete Confirmation page where you can temporarily delete the selected users.            |
| <b>More Actions &gt; Assign Roles</b>                   | Displays the Assign Roles page where you can assign roles to selected users.                               |
| <b>More Actions &gt; Add To Group</b>                   | Displays the Assign Groups page where you can assign groups to selected users.                             |
| <b>More Actions &gt; Show Deleted User</b>              | Displays the Deleted Users page where you can view, delete, or restore the deleted users.                  |
| <b>More Actions &gt; Bulk Edit Users</b>                | Displays the User Bulk Editor page where you can change the user data.                                     |
| <b>More Actions &gt; Status of Bulk Edit Users Jobs</b> | Displays the Schedule Bulk Edit of Users page where you can view or delete the bulk edit job.              |
| <b>More Actions &gt; Import Users</b>                   | Displays the Import users page where you can import the user-related data in bulk.                         |
| <b>More Actions &gt; Export All Users</b>               | Displays the Export users page where you can export the user-related data in bulk of all users.            |

*Table continues...*

| Button                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Actions &gt; Export Selected Users</b>                                      | Displays the Export users page where you can export the user-related data in bulk of selected users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>More Actions &gt; Export Delta Users</b>                                         | <p>Displays the Export users page where you can export the added, updated, or deleted user-related data for the specific delta period.</p> <p> <b>Note:</b></p> <p>The permanently deleted users login-names in the delta period are identified on the basis of audit logs of permanently deleted users in the system. Therefore, if you change the Data Retention settings for <b>LogPurgeRule</b>, the system might affect the permanently deleted users list in the exported zip file.</p> |
| <b>More Actions &gt; Import Global Settings</b>                                     | Displays the Import global settings page where you can import shared addresses, public contacts, and presence access control list (ACLs) in bulk.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>More Actions &gt; Download Excel Template</b>                                    | Navigates to the location from where you can download the Excel template that System Manager supports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Options &gt; Advanced Search</b>                                                 | Displays fields where you can specify the search criteria for searching a user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options &gt; Clear Filters</b>                                                   | Clears the filter criteria.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Filter menu</b>                                                                  | You can find the <b>Filter menu</b> icon next to the name of each column. Filters the data based on the search criteria.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Select: All</b>                                                                  | Selects all users in the table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Select: None</b>                                                                 | Clears the check box selections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|  | Refreshes the user information in the table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Criteria

Click **Advanced Search** to view this section. You can find the **Advanced Search** link in the **Options** drop-down list in the upper-right corner of the page.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>The criteria to search. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Field 1:</b> Lists the criteria that you can use to search users.</li> <li>• <b>Field 2:</b> Lists the operators for evaluating the expression. The operators displayed depends on the criterion that you selected in <b>Field 1</b>.</li> <li>• <b>Field 3:</b> Lists the value for the search criterion. The User Management service retrieves and displays users that match this value.</li> </ul> |



## User Profile | Add field descriptions

Use the User Profile | Add page to create or add a new user. This page has four tabs:

- Identity
- Communication Profile
- Membership
- Contacts

 **Note:**

Fields marked with an asterisk are mandatory, and you must enter appropriate information in these fields.

### Organization

| Name           | Description                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tenant</b>  | The name of the tenant that you select.                                                                                                                            |
| <b>Level 1</b> | The name of the level 1 hierarchy of the tenant organization. For example, Site.<br>The tenant administrator provides the hierarchy on the Tenant Management page. |
| <b>Level 2</b> | The name of the level 2 hierarchy of the tenant organization. For example, Department.                                                                             |
| <b>Level 3</b> | The name of the level 3 hierarchy of the tenant organization. For example, Team.                                                                                   |

### User Provisioning Rule

| Name                          | Description                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------|
| <b>User Provisioning Rule</b> | The name of the user provisioning rule.<br>You can provide only one user provisioning rule. |

 **Note:**

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

### Identity tab: Identity

| Name             | Description                                     |
|------------------|-------------------------------------------------|
| <b>Last Name</b> | The last name of the user. For example, Miller. |

*Table continues...*

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p> <b>Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>• Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>• Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the user. For example, John.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Middle Name</b>                    | The middle name of the user, if any.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                    | A brief description of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

*Table continues...*

| Name                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Login Name</b>    | <p>The login name of the user.</p> <p>With Release 8.1.3, the <b>Login Name</b> field supports the login name with apostrophe ('). For example, aine'mars@xyz.com.</p> <p>The following characters are supported:</p> <ul style="list-style-type: none"> <li>• ,</li> <li>• -</li> <li>• _</li> <li>• ?</li> <li>• %</li> <li>• !</li> <li>• ~</li> <li>• *</li> <li>• (</li> <li>• )</li> <li>• =</li> <li>• +</li> <li>• \$</li> <li>• ,,</li> <li>• ;</li> <li>• .</li> <li>• '.</li> </ul> <p>The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter the login name in uppercase or lowercase.</p> <p>If you log in to the system as admin, you cannot edit the login name.</p> <p> <b>Note:</b></p> <p>To create the user data by using a blank excel template, append the login name with #ProfileSetName in all worksheets, except Basic and Profile Set. The system associates the user records with the communication profile that you have provided. For example, jmiller@avaya.com#ProfileSetName.</p> |
| <b>Email Address</b> | The email address of the user for receiving email notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Type</b>              | <p>The authentication type that defines how the system authenticates the user. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Enterprise</b>: Directory servers that are external to System Manager authenticate the user login.</li> <li>• <b>Basic</b>: Avaya authentication service authenticates the user login.</li> </ul> <p>For bulk import of users by using Excel, <b>User Type</b> is always Basic. Therefore, the <b>User Type</b> field remains invisible in the Excel file.</p> |
| <b>Password</b>               | The password to log in to the System Manager web console.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Confirm Password</b>       | The password that you reenter for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Localized Display Name</b> | The localized display name of a user. The name is typically the localized full name.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Title</b>                  | The personal title that is set to address a user. The title is typically a social title and not the work title. For example, Mr.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Language Preference</b>    | The preferred written or spoken language of the user. For example, English.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Time Zone</b>              | The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Employee ID</b>            | The employee number of the user. For example, 20081234.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Department</b>             | The department to which the user belongs. For example, Human Resources.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Company</b>                | The organization where the user works. For example, Avaya Inc.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

### Identity tab: Address

| Name                    | Description                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b> | The option to select an address in the table.                                                                                                    |
| <b>Name</b>             | The name of the addressee. For example, Avaya.                                                                                                   |
| <b>Address Type</b>     | <p>The type of address. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Office</b></li> <li>• <b>Home</b></li> </ul>            |
| <b>Street</b>           | The name of the street. For example, Magarpatta.                                                                                                 |
| <b>City</b>             | The name of the city or town. For example, Pune.                                                                                                 |
| <b>Postal Code</b>      | The postal code used by postal services to route mail to a destination. For example, 411028. For United States, the postal code is the Zip code. |
| <b>Province</b>         | The full name of the province. For example, Maharashtra.                                                                                         |
| <b>Country</b>          | The name of the country. For example, India.                                                                                                     |

| Button                       | Description                                                              |
|------------------------------|--------------------------------------------------------------------------|
| <b>New</b>                   | Displays the Add Address page to add the address details.                |
| <b>Edit</b>                  | Displays the Edit Address page to modify the address.                    |
| <b>Delete</b>                | Deletes the selected address.                                            |
| <b>Choose Shared Address</b> | Displays the Choose Address where you choose a shared or common address. |

## Identity tab: Localized Names

### \* Note:

Use the **Localized Names** section only for the CS 1000 system, not for Session Manager and Communication Manager.

| Name                | Description                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------|
| <b>Language</b>     | The localized language for displaying the user name. For example, English. You must select the language. |
| <b>Display Name</b> | The user name in the localized language you choose. For example, John Miller.                            |

| Button        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| <b>New</b>    | Displays fields that you can use to create a new localized name for the user. |
| <b>Edit</b>   | Displays fields that you can use to modify the localized name of the user.    |
| <b>Delete</b> | Deletes the localized names that you select for the user.                     |
| <b>Add</b>    | Adds or edits the localized name of the user.                                 |
| <b>Cancel</b> | Cancels the addition or edits of the localized name.                          |

## Communication Profile tab: Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Communication Profile Password</b> | <p>The communication profile password.</p> <p>The field is available only if you enable the communication profile. The password policy is configured on the <b>Users &gt; User Management &gt; Communication Profile Password Policy</b> page.</p> <p>When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user.</p> <p>For information about password policy, see “Communication profile password policy”.</p> |
| <b>Confirm Password</b>               | The communication profile password that you reenter for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generate</b> | <p>The option to automatically generate the communication profile password.</p> <p>System Manager sends the generated password to the user if you:</p> <ul style="list-style-type: none"> <li>Set the email configuration properties on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR</b> page.</li> </ul> <p>For more information, see “Configuring email properties”.</p> <ul style="list-style-type: none"> <li>Configure <b>Email Address</b> on the <b>Identity</b> tab.</li> </ul> <p>By default, the <b>Generate</b> link is available for creating a new user account.</p> <p>The <b>Edit</b> link is available for modifying user accounts. When you click the <b>Edit</b> link, the system displays <b>Confirm Password</b> along with the <b>Generate</b> and <b>Cancel</b> links.</p> |
| <b>Name</b>     | The name of the communication profile that you must select .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.                                          |
| <b>Done</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancels the operation of adding a communication profile.                             |

The system enables the following fields when you click **New** in the **Communication Profile** section.

| Name           | Description                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>    | The name of the communication profile for the user.                                                                          |
| <b>Default</b> | <p>The option to select a profile as default or the active profile.</p> <p>At a time, only one active profile can exist.</p> |

### Communication Profile tab: Communication Address

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

| Name          | Description                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>   | The type of handle.                                                                                                          |
| <b>Handle</b> | A unique communication address of the user. Communication Manager Release 7.1.2 and later also support alphanumeric handles. |
| <b>Domain</b> | The name of the domain with which the handle is registered.                                                                  |

| Button     | Description                         |
|------------|-------------------------------------|
| <b>New</b> | To add a new communication address. |

*Table continues...*

| Button        | Description                                                  |
|---------------|--------------------------------------------------------------|
| <b>Edit</b>   | To edit the information of a selected communication address. |
| <b>Delete</b> | To delete the selected communication address.                |

When you click **New** and **Edit** in the Communication Address section, the page displays the following fields that define the communication address of the user:

| Name        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b> | <p>The type of handle. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Avaya SIP</b>: Indicates that the handle supports Avaya SIP-based communication.</li> <li>• <b>Avaya E.164</b>: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have maximum 13 digits and are usually written with a + prefix.</li> <li>• <b>Microsoft SIP</b>: Indicates that the handle supports SIP-based communication.</li> <li>• <b>Microsoft Exchange</b>: Indicates that the handle is an email address and supports communication with Microsoft SMTP server.</li> <li>• <b>Lotus Notes</b>: Indicates that the handle is for Lotus Notes and domino calendar.</li> <li>• <b>IBM Sametime</b>: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format.</li> <li>• <b>Avaya Presence/IM</b>: Indicates that the handle is an address that is used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services and XMPP or Session Initiation Protocol-based (SIP) Presence services.</li> </ul> <p> <b>Note:</b></p> <p>To create the Presence communication profile, you must select <b>Avaya Presence/IM</b> and provide the communication address.</p> <ul style="list-style-type: none"> <li>• <b>GoogleTalk</b>: Indicates that the handle supports XMPP-based communication with the Google Talk service.</li> <li>• <b>Other Email</b>: Indicates that the handle is an email address other than MS Exchange email addresses.</li> <li>• <b>Other SIP</b>: Indicates that the handle supports SIP-based communication other than the listed ones.</li> <li>• <b>Other XMPP</b>: Indicates that the handle supports XMPP-based communication other than the listed ones.</li> <li>• <b>Work Assignment</b>: Indicates that the handle supports accounts that can be assigned to an agent for Work Assignment.</li> </ul> |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fully Qualified Address</b> | The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address. |

| Button        | Description                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------|
| <b>Add</b>    | Saves the new communication address or modified communication address information in the database. |
| <b>Cancel</b> | Cancels the addition of communication address.                                                     |

### Communication Profile tab: Session Manager

 **Note:**

The system displays the following fields only if a communication profile of the user exists for the product:

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Session Manager</b>   | The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura <sup>®</sup> network. You must select the primary Session Manager server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Secondary Session Manager</b> | The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Survivability Server</b>      | <p>For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.</p> <p> <b>Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.</p> <p>After typing minimum of 3 characters, wait for three seconds to capture the final keyword, and fetch the required results.</p> |

*Table continues...*



| Name                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max. Simultaneous Devices</b>                                | The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Block New Registration When Maximum Registrations Active</b> | <p>If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.</p> <p>If you clear the check box, the system accepts the new registration and unregisters the endpoint with the oldest registration. However, if the endpoint with the oldest registration is active on a call, then the system does not unregister the endpoint until the call is completed.</p> |
| <b>Origination Application Sequence</b>                         | <p>The application sequence that the system invokes when routing calls from this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p>                                                                                                                                                                                |
| <b>Termination Application Sequence</b>                         | <p>The application sequence that is invoked when the system routes calls to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p>                                                                                                                                                                               |
| <b>Emergency Calling Origination Sequence</b>                   | The list of application sequences invoked when the system routes emergency calls from this user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Emergency Calling Termination Sequence</b>                   | The list of application sequences invoked when the system routes emergency calls to this user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Home Location</b>                                            | The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any location. You must specify a value.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Conference Factory Set</b>                                   | <p>The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.</p> <p>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.</p>                                                                                                                                                                                                                                                                                                                                                |
| <b>Enable Centralized Call History</b>                          | <p>The option to enable the call history feature for SIP users.</p> <p>By default, the system disables the call history feature. The maximum number of call logs per communication profile is 100.</p>                                                                                                                                                                                                                                                                                                                                                                                                             |

**Communication Profile tab: Avaya Breeze® platform Profile**

| Name                   | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Service Profile</b> | The profile that you assign to the user. The user can gain access to the service contained in the profile. |

**Communication Profile tab: CM Endpoint Profile****\* Note:**

The system displays these fields only if a Communication Manager Endpoint profile exists for the user.

| Name                          | Description                                                                                                                                                                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                 | The Communication Manager system on which you add the endpoint. You must select the system.                                                                                                                                                                                                                    |
| <b>Profile Type</b>           | The type of Communication Manager Endpoint profile that you create. You must select the profile type.                                                                                                                                                                                                          |
| <b>Use Existing Endpoints</b> | The existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.                                                                                                                                                                 |
| <b>Extension</b>              | The extension of the endpoint that you associate this profile with. You must select the extension.<br><br>The field lists the endpoints, existing or available, based on the option you selected in the <b>Use Existing Endpoints</b> check box.                                                               |
| <b>Endpoint Editor</b> button | To start the Communication Manager application where you can edit or view details of the endpoint.<br><br>After you save the changes in Communication Manager, the system updates the modified data on the device or database only after you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Template</b>               | The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add.                                                                                                                                                                         |
| <b>Set Type</b>               | The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.                                                                                                                                                                                 |
| <b>Sub Type</b>               | This field is configured for CS 1000 station types only. You can select the specific set for <b>Set Type</b> . On the Manage Endpoint page, <b>Sub Type</b> is labeled as <b>Set</b> .                                                                                                                         |
| <b>Terminal Number</b>        | This field is configured for CS 1000 station types only. You can enter numbers in the following range: 0.0.0.0 to 252.1.15.31.<br><br>The first digit must be divisible by 4. For example: 0, 4, 8, ..., 252.                                                                                                  |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System ID</b>               | <p>This field is configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0 more than one station can use the combination of <b>System ID</b> and <b>Terminal Number</b>.</p> <p>With Release 8.0.1, each station must have a unique combination of <b>System ID</b> and <b>Terminal Number</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Security Code</b>           | The security code for authorized access to the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Port</b>                    | <p>The relevant port for the set type you select. You must select the port.</p> <p>The field lists the possible ports based on the selected set type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Voice Mail Number</b>       | <p>The voice mail number of the endpoint you associate with.</p> <p> <b>Note:</b></p> <p>You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of <b>Voice Mail Number</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Preferred Handle</b>        | <p>Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user.</p> <p>The <b>Preferred Handle</b> field is optional. Select numeric handle for alphanumeric support. By default, the field is blank.</p> <p>If the type of SIP entity is Communication Manager, Session Manager uses the preferred handle in the CM Endpoint profile. By default, for a SIP station, Communication Manager uses the extension number as the phone number entry on an OPS station-mapping table. If your enterprise dial plan has SIP handles that are different from the Communication Manager extension, then use the <b>Preferred Handle</b> field to change the phone number entry on the OPS station-mapping table on the Communication Manager.</p> <p>To modify the phone number entry, the Communication Address in System Manager should have a SIP handle. In the CM Endpoint Communication Profile, set the <b>Preferred Handle</b> field to the SIP handle format. After you click <b>Commit</b>, System Manager sets the <b>Phone Number</b> field in the OPS station-mapping table on Communication Manager to the SIP handle format. If you do not need this feature, then set the <b>Preferred Handle</b> value to <b>None</b>.</p> |
| <b>Calculate Route Pattern</b> | The option to automatically select the route pattern based on the primary or secondary Session Manager configured in <b>Session Manager Communication Profile</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Sip Trunk</b>               | <p>The system makes this field available only for the SIP set type.</p> <p>If you select the <b>Calculate Route Pattern</b> check box, the system:</p> <ul style="list-style-type: none"> <li>• Populates the <b>Sip Trunk</b> field.</li> <li>• Makes the <b>Sip Trunk</b> field read-only.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP URI</b>                                                             | A unique alphanumeric communication address of the user to make and receive voice or video calls. The <b>SIP URI</b> address can be: <username-projectname>@<xyz.com>.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Attendant</b>                                                           | The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.<br><br>When you select the 9641SIP template type from <b>Template</b> , the system enables the <b>Attendant</b> check box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Enhanced Callr-Info display for 1-line phones</b>                       | The option to activate the enhanced Callr-info operation on the phone.<br><br>The <b>Enhanced Callr-Info display for 1-line phones</b> field on the station form is valid for the following set types: <ul style="list-style-type: none"> <li>• 1603, 1608, 1616, 1408, 1416</li> <li>• 2402, 2410, 2420</li> <li>• 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625,</li> <li>• 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1</li> <li>• 7506D, 7507D</li> <li>• 8405D+, 8410D, 8405D, 8411D</li> <li>• 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650</li> </ul> The options are: <ul style="list-style-type: none"> <li>• <b>No</b>: Does not change the callr-info interactions with the connected phone. The default setting.</li> <li>• <b>Yes</b>: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call, and on-call-release. If the <b>callr-info</b> button is not assigned to the phone on the station form, <b>Enhanced Callr-Info display for 1-line phones</b> does not apply.</li> </ul> |
| <b>Delete Endpoint on Unassign of Endpoint from User or on Delete User</b> | The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or delete the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

*Table continues...*

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Override Endpoint Name and Localized Name</b>      | <p>The option to override the following endpoint names:</p> <ul style="list-style-type: none"> <li>The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization.</li> </ul> <p>If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization.</p> <ul style="list-style-type: none"> <li>The localized display name on the Manage Users page in the <b>Localized Display Name</b> field of Communication Manager. If you clear the check box, the system does not override the localized display name in the <b>Localized Display Name</b> field.</li> </ul> |
| <b>Allow H.323 and SIP Endpoint Dual Registration</b> | <p>The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</p>                                                                                                                                                                                                                                                                                                                                                     |

### Communication Profile tab: CS 1000 Endpoint Profile

| Name                   | Description                                                                                                                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>          | The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.                                                                                                                   |
| <b>Add new</b>         | The option to create a new phone.                                                                                                                                                                                          |
| <b>Target</b>          | <p>The system customer number of the CS 1000 system. You must select the target.</p> <p>The system displays the field only when you select <b>Add new</b>.</p>                                                             |
| <b>Template</b>        | <p>The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.</p> <p>The system displays the field only when you select <b>Add new</b>.</p> |
| <b>Update</b>          | The station profile information updated for the user. When you click <b>Update</b> , the system takes you to the element manager cut-through for the updates.                                                              |
| <b>Service Details</b> | The service details of endpoints, such as set type, after phone creation.                                                                                                                                                  |
| <b>Primary DN</b>      | <p>The primary directory number of the phone. You can enter only numeric values in this field.</p> <p>The system displays the field only when you select <b>Add new</b>.</p>                                               |
| <b>Terminal Number</b> | <p>The terminal number of the phone.</p> <p>The system displays the field only when you select <b>Add new</b>.</p>                                                                                                         |
| <b>Link existing</b>   | The option to associate with the existing phone.                                                                                                                                                                           |
| <b>Existing TN</b>     | <p>The terminal number from the list of existing numbers.</p> <p>The system displays the field only when you select <b>Link existing</b>.</p>                                                                              |

Table continues...

| Name                                  | Description                                                                |
|---------------------------------------|----------------------------------------------------------------------------|
| <b>Include in Corporate Directory</b> | The option to add this profile to the CS 1000 Corporate Directory feature. |

### Communication Profile tab: Messaging Profile

**\* Note:**

The system displays the following fields only if you can configure a messaging profile for the user

| Name                                                                           | Description                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                                                  | The messaging system on which you add the subscriber. You must select the system.                                                                                                                                                                                                                                    |
| <b>Use Existing Subscriber on System</b>                                       | The option to specify whether to use an existing subscriber mailbox number to associate with this profile.                                                                                                                                                                                                           |
| <b>Mailbox Number</b>                                                          | The mailbox number of the subscriber. You must select the mailbox number.<br><br>The field takes the existing mailbox number that you associate with this profile. The value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                                        |
| <b>Messaging Editor</b>                                                        | The Messaging application where you can edit or view details of the profile of the messaging endpoint.<br><br>After you save the changes in the Messaging system, the system does not update the modified data on the device or database until you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Template</b>                                                                | The system-defined or user-defined template that you associate with the subscriber.                                                                                                                                                                                                                                  |
| <b>Password</b>                                                                | The password for logging in to the mailbox. You must provide the password.                                                                                                                                                                                                                                           |
| <b>Delete Subscriber on Unassign of Subscriber from User or on Delete User</b> | The option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this Messaging profile or delete the user.                                                                                                                               |

### Communication Profile tab: Avaya Messaging Profile

| Name                     | Description                                                                                                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Officelinx System</b> | The Avaya Messaging system to which you add a mailbox.                                                                                                                                                    |
| <b>Refresh</b>           | The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use.<br><br>You do not require to refresh for every user. |
| <b>Mailbox Number</b>    | The mailbox number of the subscriber.                                                                                                                                                                     |

*Table continues...*

| Name                                     | Description                                                                                                                                                                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Numeric Password</b>                  | The numeric password that is used to log in to the Avaya Messaging system.                                                                                                                                                                                            |
| <b>Confirm Numeric Password</b>          | The numeric password that you retype to confirm.                                                                                                                                                                                                                      |
| <b>Application User Password</b>         | The password that is used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.                                                                                                                       |
| <b>Confirm Application User Password</b> | The password that you retype to confirm.                                                                                                                                                                                                                              |
| <b>Company</b>                           | The name of the company to which the user belongs.                                                                                                                                                                                                                    |
| <b>Department</b>                        | The department to which the user belongs.                                                                                                                                                                                                                             |
| <b>Feature Group</b>                     | The feature group name that determines the rules for the mailboxes associated with it.                                                                                                                                                                                |
| <b>Capability</b>                        | The type of functionality that the user contains. The values are: <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Fax</b></li> <li>• <b>Messaging</b></li> <li>• <b>Collaboration</b></li> <li>• <b>Messaging and Collaboration</b></li> </ul> |
| <b>Domain Account Name</b>               | The mailbox NT account name of the Avaya Messaging profile.                                                                                                                                                                                                           |
| <b>Synchronization User Name</b>         | The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.                                                                                                                                                   |

**\* Note:**

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

### Communication Profile tab: IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

**\* Note:**

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Before you add an IP Office endpoint profile for a centralized user, commit the changes to the Communication Manager endpoint profile and the Session Manager endpoint profile.

| Name                                   | Description                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                          | The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.                                                                                                                                                             |
| <b>Template</b>                        | The list of user templates from which you can select your preferred template to set the user configurations. You must select the template.                                                                                                                                                                    |
| <b>Use Existing Extension</b>          | Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.                                                                                                                                     |
| <b>Extension</b>                       | The extension of the endpoint you associate with. You must select the extension.<br><br>The field lists the endpoints, existing or available, based on the option you selected in the <b>Use Existing Endpoints</b> check box.                                                                                |
| <b>Endpoint Editor</b>                 | Starts the IP Office application where you can edit or view the details of the IP Office endpoint.<br><br>After you save the changes in the IP Office manager, the system updates the modified data on the device or database only when you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Module-Port</b>                     | The module port combination list for IP Office analog extensions. You must select <b>Module-Port</b> for centralized users with Set Type as <b>Analog</b> .                                                                                                                                                   |
| <b>Set Type</b>                        | The set type for the IP Office endpoint profile. By default, the <b>Set Type</b> field is disabled. If you select a template, the system populates the set type.                                                                                                                                              |
| <b>Delete Extension On User Delete</b> | The option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with <b>Analog</b> and <b>Digital</b> set types.                                                                     |

### Communication Profile tab: Equinox Conferencing

| Name                         | Description                                  |
|------------------------------|----------------------------------------------|
| <b>Equinox User Password</b> | The Equinox user password.                   |
| <b>Virtual Room Number</b>   | The virtual room number of the Equinox user. |

### Communication Profile tab: Presence Profile

You can create Presence profiles only for the default communication profile.

| Name          | Description                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b> | The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: <ul style="list-style-type: none"> <li>Aggregate presence</li> <li>Archive instant messages if the Instant Messages option is enabled</li> </ul> |

*Table continues...*



| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SIP Entity</b>                          | The option to route the SIP-based messages through Presence Services.<br><br>This system selects the SIP entity only if you select a Presence Services instance in the <b>System</b> field. <b>SIP Entity</b> is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.                                                         |
| <b>IM Gateway SIP Entity</b>               | The Presence Services instance for the user.                                                                                                                                                                                                                                                                                                                                            |
| <b>Publish Presence with AES Collector</b> | The option that determines if Presence Services must publish presence with AES Collector. The options are: <ul style="list-style-type: none"> <li>• <b>System Default</b></li> <li>• <b>Off</b></li> <li>• <b>On</b></li> </ul> The default is <b>System Default</b> . You can change the default value. You do not require to configure AES Collector in the Presence Services server. |

### Communication Profile tab: Conferencing Profile

| Name                                                         | Description                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Auto-generated Code Length</b>                     | The number of characters in PIN. The default is 6.<br><br>The system displays this field if you select the <b>Auto Generate Participant and Moderator Security Code</b> check box.                                                                             |
| <b>Auto Generate Participant and Moderator Security Code</b> | Select the check box if the system must generate the participant security code and moderator security code for this user.<br><br>Clear the check box to assign a specific participant security code or moderator security code for this user.                  |
| <b>Participant Security Code</b>                             | The participant security code that you assign for this user.<br><br>The system displays this field only when the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.                                                              |
| <b>Moderator Security Code</b>                               | The moderator security code that you assign for this user.<br><br>The system displays this field if the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.                                                                       |
| <b>Location</b>                                              | The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.<br><br>For SIP users, the system uses the location value from the <b>Home Location</b> field in the Session Manager profile. |
| <b>Template</b>                                              | The Conferencing template that you assign to this user.                                                                                                                                                                                                        |

| Button               | Description                                                                     |
|----------------------|---------------------------------------------------------------------------------|
| <b>Get Templates</b> | Displays the list of Conferencing templates, which you can assign to this user. |

**Communication Profile tab: Work Assignment Profile**

| Name                   | Description          |
|------------------------|----------------------|
| <b>Account</b>         | The account name.    |
| <b>Account Address</b> | The account address. |
| <b>Source</b>          | The source name.     |
| <b>Source Address</b>  | The source address.  |

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

| Button                  | Description                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Resource Details</b> | Displays the Assignment Management page where you can configure assignment targets for the user.<br><br>You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user. |
| <b>Account Details</b>  | Displays the text box where you can add or modify the account name and account address.<br><br>You can add attributes to the account only when the account is added to the agent.                                            |
| <b>Source Details</b>   | Displays the text box where you can add or modify the source name and source address.<br><br>You can add properties and attributes to the source only when the source already exists.                                        |

**Membership tab: Roles**

| Name                    | Description                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b> | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| <b>Name</b>             | The name of the role.                                                                                                                                        |
| <b>Description</b>      | A brief description about the role.                                                                                                                          |

| Button                | Description                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------|
| <b>Assign Roles</b>   | Displays the Assign Role page that you can use to assign the roles to the user account. |
| <b>Unassign Roles</b> | Removes the selected role from the list of roles associated with the user account.      |

**Membership tab: Group Membership**

| Name                    | Description                                 |
|-------------------------|---------------------------------------------|
| <b>Select check box</b> | Use this check box to select a group.       |
| <b>Name</b>             | The name of the group.                      |
| <b>Type</b>             | The group type based on the resources.      |
| <b>Hierarchy</b>        | The position of the group in the hierarchy. |
| <b>Description</b>      | A brief description about the group.        |

| Button                   | Description                                                                  |
|--------------------------|------------------------------------------------------------------------------|
| <b>Add To group</b>      | Displays the Assign Groups page that you can use to add the user to a group. |
| <b>Remove From Group</b> | Removes the user from the selected group.                                    |

**Contacts tab: Default Contact List**

| Name               | Description                              |
|--------------------|------------------------------------------|
| <b>Description</b> | A brief description of the contact list. |

**Contacts tab: Associated Contacts**

| Name                    | Description                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>        | The last name of the contact.                                                                                                                                          |
| <b>First Name</b>       | The first name of the contact.                                                                                                                                         |
| <b>Scope</b>            | The categorization of the contact based on whether the contact is a public or private contact.                                                                         |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.                                                                                              |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.                                                                                                              |
| <b>Presence Buddy</b>   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you cannot track the presence of the contact. |

| Button      | Description                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact. |

*Table continues...*

| Button             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Add</b>         | Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.<br><br>In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts: <ul style="list-style-type: none"> <li>• Private contacts of the user</li> <li>• Public contacts</li> <li>• Users who belong to that tenant</li> </ul> |
| <b>Remove</b>      | Removes one or more selected contacts from the list of the associated contacts.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Filter menu</b> | You can find the <b>Filter menu</b> icon next to the name of each column.<br><br>Filters the data based on the search criteria.                                                                                                                                                                                                                                                                                                             |

### Contacts tab: Private Contacts

Use this section to add new private contacts, and edit and delete the existing contacts.

| Name                   | Description                              |
|------------------------|------------------------------------------|
| <b>Last Name</b>       | The last name of the private contact.    |
| <b>First Name</b>      | The first name of the private contact.   |
| <b>Display Name</b>    | The display name of the private contact. |
| <b>Contact Address</b> | The address of the private contact.      |
| <b>Description</b>     | A brief description about the contact.   |

| Button             | Description                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>        | Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.                      |
| <b>New</b>         | Displays the <b>New Private Contact</b> page. Use this page to add a new private contact.                                       |
| <b>Delete</b>      | Deletes the selected contacts.                                                                                                  |
| <b>Filter menu</b> | You can find the <b>Filter menu</b> icon next to the name of each column.<br><br>Filters the data based on the search criteria. |

### Common buttons

| Button                       | Description                                                                                          |
|------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Commit &amp; Continue</b> | Creates the user account in the database and retains you on the same page for further modifications. |
| <b>Commit</b>                | Creates the user account and takes you to the User Management page.                                  |
| <b>Cancel</b>                | Cancels the user creation operation.                                                                 |

## Related links

[Communication profile password policy](#) on page 609

## User Profile | Edit | <User Name> field descriptions

### Organization

| Name           | Description                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tenant</b>  | The name of the tenant that you select.                                                                                                                                |
| <b>Level 1</b> | The name of the level 1 hierarchy of the tenant organization. For example, Site.<br><br>The tenant administrator provides the hierarchy on the Tenant Management page. |
| <b>Level 2</b> | The name of the level 2 hierarchy of the tenant organization. For example, Department.                                                                                 |
| <b>Level 3</b> | The name of the level 3 hierarchy of the tenant organization. For example, Team.                                                                                       |

 **Note:**

You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.

### User Provisioning Rule

| Name                          | Description                                    |
|-------------------------------|------------------------------------------------|
| <b>User Provisioning Rule</b> | The user provisioning rule that you must edit. |

### Identity tab — Identity section

| Name             | Description                                     |
|------------------|-------------------------------------------------|
| <b>Last Name</b> | The last name of the user. For example, Miller. |

*Table continues...*

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p> <b>Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>• Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>• Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the user. For example, John.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Middle Name</b>                    | The middle name of the user, if any.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                    | A brief description of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Status</b>                         | The login status of the user                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Update Time</b>                    | The time when the user details were last modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

*Table continues...*

| Name                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Login Name</b>    | <p>The login name of the user.</p> <p>With Release 8.1.3, the <b>Login Name</b> field supports the login name with apostrophe ('). For example, aine'mars@xyz.com.</p> <p>The following characters are supported:</p> <ul style="list-style-type: none"> <li>• ,</li> <li>• -</li> <li>• _</li> <li>• ?</li> <li>• %</li> <li>• !</li> <li>• ~</li> <li>• *</li> <li>• (</li> <li>• )</li> <li>• =</li> <li>• +</li> <li>• \$</li> <li>• ,,</li> <li>• ;</li> <li>• .</li> <li>• '.</li> </ul> <p>The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter the login name in uppercase or lowercase.</p> <p>If you log in to the system as admin, you cannot edit the login name.</p> <p> <b>Note:</b></p> <p>To create the user data by using a blank excel template, append the login name with #ProfileSetName in all worksheets, except Basic and Profile Set. The system associates the user records with the communication profile that you have provided. For example, jmiller@avaya.com#ProfileSetName.</p> |
| <b>Email Address</b> | The email address of the user                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Type</b>              | The authentication type that defines how the system authenticates the user. The options are: <ul style="list-style-type: none"> <li>• <b>Enterprise</b>: Directory servers that are external to System Manager authenticate the user login.</li> <li>• <b>Basic</b>: Avaya authentication service authenticates the user login.</li> </ul> For bulk import of users by using Excel, <b>User Type</b> is always Basic. Therefore, the <b>User Type</b> field remains invisible in the Excel file. |
| <b>Change Password</b>        | Displays two new fields: <b>New Password</b> and <b>Confirm Password</b> .                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>New Password</b>           | The new password to log in to the System Manager web console.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Confirm Password</b>       | The password that you reenter for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Source</b>                 | The entity that created this user record. The possible values for this field is either an IP Address/Port, or a name representing an enterprise LDAP, or Avaya.                                                                                                                                                                                                                                                                                                                                  |
| <b>Localized Display Name</b> | The localized display name of a user. The name is typically the localized full name.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. The display name supports displays that cannot handle localized text, for example, some endpoints.                                                                                                                                                                                                                                                                                                                                          |
| <b>Title</b>                  | The personal title that is set to address a user. The title is typically a social title and not the work title. For example, Mr.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Language Preference</b>    | The preferred written or spoken language of the user. For example, English.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Time Zone</b>              | The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Employee ID</b>            | The employee number of the user. For example, 20081234.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Department</b>             | The department to which the user belongs. For example, Human Resources.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Company</b>                | The organization where the user works. For example, Avaya Inc.                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Identity tab — Address section

| Name                | Description                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Zone</b>    | The preferred time zone of the user. For example, (+05:30) Chennai, Kolkata, Mumbai, New Delhi.                                |
| <b>Department</b>   | The department to which the user belongs. For example, Human Resources.                                                        |
| <b>Address Type</b> | The type of address. The options are: <ul style="list-style-type: none"> <li>• <b>Office</b></li> <li>• <b>Home</b></li> </ul> |
| <b>Street</b>       | The name of the street. For example, Magarpatta.                                                                               |

*Table continues...*



| Name               | Description                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>City</b>        | The name of the city or town. For example, Pune.                                                                                                 |
| <b>Postal Code</b> | The postal code used by postal services to route mail to a destination. For example, 411028. For United States, the postal code is the Zip code. |
| <b>Province</b>    | The full name of the province. For example, Maharashtra.                                                                                         |
| <b>Country</b>     | The name of the country. For example, India.                                                                                                     |

| Button                       | Description                                                              |
|------------------------------|--------------------------------------------------------------------------|
| <b>New</b>                   | Displays the Add Address page to add the address details.                |
| <b>Edit</b>                  | Displays the Edit Address page to modify the address.                    |
| <b>Delete</b>                | Deletes the selected address.                                            |
| <b>Choose Shared Address</b> | Displays the Choose Address where you choose a shared or common address. |

### Identity tab — Localized Names section

| Name                | Description                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------|
| <b>Language</b>     | The localized language for displaying the user name. For example, English. You must select the language. |
| <b>Display Name</b> | The user name in the localized language you choose. For example, John Miller.                            |

| Button        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| <b>New</b>    | Displays fields that you can use to create a new localized name for the user. |
| <b>Edit</b>   | Displays fields that you can use to modify the localized name of the user.    |
| <b>Delete</b> | Deletes the localized names that you select for the user.                     |
| <b>Add</b>    | Adds or edits the localized name of the user.                                 |
| <b>Cancel</b> | Cancels the addition or edits of the localized name.                          |

### Communication Profile tab — Communication Profile

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

| Name                           | Description                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Calculate Route Pattern</b> | The option to automatically select the route pattern based on the primary or secondary Session Manager configured in the <b>Session Manager Communication Profile</b> .                                             |
| <b>Sip Trunk</b>               | The system makes this field available only for the SIP set type.<br><br>If you select the <b>Calculate Route Pattern</b> check box, the system populates the <b>Sip Trunk</b> field, and makes the field read-only. |

*Table continues...*

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Allow H.323 and SIP Endpoint Dual Registration</b> | The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a> . |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.                                          |
| <b>Done</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancels the operation of adding a communication profile.                             |

The system enables the following fields when you click **New** in the Communication Profile section.

| Name           | Description                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------|
| <b>Name</b>    | The name of the communication profile for the user.                                                     |
| <b>Default</b> | The profile that is made default as the active profile. There can be only one active profile at a time. |

### Communication Profile tab — Communication Address

Use this section to create, modify, and delete the communication address of a user. Each communication profile can contain one or more communication addresses for a user.

| Name          | Description                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>   | The type of handle.                                                                                                          |
| <b>Handle</b> | A unique communication address of the user. Communication Manager Release 7.1.2 and later also support alphanumeric handles. |
| <b>Domain</b> | The name of the domain with which the handle is registered.                                                                  |

| Button        | Description                                                  |
|---------------|--------------------------------------------------------------|
| <b>New</b>    | To add a new communication address.                          |
| <b>Edit</b>   | To edit the information of a selected communication address. |
| <b>Delete</b> | To delete the selected communication address.                |

The page displays the following fields when you click **New** or **Edit** in the Communication Address section.

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>                    | <p>The type of handle. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Avaya SIP</b>: Indicates that the handle supports Avaya SIP-based communication.</li> <li>• <b>Avaya E.164</b>: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have maximum 13 digits and are usually written with a + prefix.</li> <li>• <b>Microsoft SIP</b>: Indicates that the handle supports SIP-based communication.</li> <li>• <b>Microsoft Exchange</b>: Indicates that the handle is an email address and supports communication with Microsoft SMTP server.</li> <li>• <b>Lotus Notes</b>: Indicates that the handle is for Lotus Notes and domino calendar.</li> <li>• <b>IBM Sametime</b>: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format.</li> <li>• <b>Avaya Presence/IM</b>: Indicates that the handle is an address that is used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services and XMPP or Session Initiation Protocol-based (SIP) Presence services.</li> </ul> <p> <b>Note:</b></p> <p>To create the Presence communication profile, you must select <b>Avaya Presence/IM</b> and provide the communication address.</p> <ul style="list-style-type: none"> <li>• <b>GoogleTalk</b>: Indicates that the handle supports XMPP-based communication with the Google Talk service.</li> <li>• <b>Other Email</b>: Indicates that the handle is an email address other than MS Exchange email addresses.</li> <li>• <b>Other SIP</b>: Indicates that the handle supports SIP-based communication other than the listed ones.</li> <li>• <b>Other XMPP</b>: Indicates that the handle supports XMPP-based communication other than the listed ones.</li> <li>• <b>Work Assignment</b>: Indicates that the handle supports accounts that can be assigned to an agent for Work Assignment.</li> </ul> |
| <b>Fully Qualified Address</b> | The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Button        | Description                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------|
| <b>Add</b>    | Saves the new communication address or modified communication address information in the database. |
| <b>Cancel</b> | Cancels the addition of communication address.                                                     |

**Communication Profile tab:— Session Manager****\* Note:**

The system displays the following fields only if a communication profile of the user exists for the product:

| Name                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Session Manager</b>                                  | The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura <sup>®</sup> network. You must select the primary Session Manager server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Secondary Session Manager</b>                                | The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Survivability Server</b>                                     | <p>For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.</p> <p><b>* Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.</p> <p>After typing minimum of 3 characters, wait for three seconds to capture the final keyword, and fetch the required results.</p> |
| <b>Max. Simultaneous Devices</b>                                | The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Block New Registration When Maximum Registrations Active</b> | If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Origination Application Sequence</b> | <p>The application sequence that the system invokes when routing calls from this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> |
| <b>Termination Application Sequence</b> | <p>The application sequence that is invoked when the system routes calls to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> |
| <b>Home Location</b>                    | <p>The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any location. You must specify a value.</p>                                                                                                                                                                        |
| <b>Conference Factory Set</b>           | <p>The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.</p> <p>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.</p>                                                                                                                                                                 |

### Communication Profile tab: Avaya Breeze® platform Profile

| Name                   | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Service Profile</b> | The profile that you assign to the user. The user can gain access to the service contained in the profile. |

### Communication Profile tab — CM Endpoint Profile

 **Note:**

The system displays these fields only if a Communication Manager Endpoint profile exists for the user.

| Name/Button                   | Description                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                 | The Communication Manager system on which you add the endpoint. You must select the system.                                                    |
| <b>Profile Type</b>           | The type of Communication Manager Endpoint profile that you create. You must select the profile type.                                          |
| <b>Use Existing Endpoints</b> | The existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions. |

*Table continues...*

| Name/Button              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Extension</b>         | <p>The extension of the endpoint that you associate this profile with. You must select the extension.</p> <p>The field lists the endpoints, existing or available, based on the option you selected in the <b>Use Existing Endpoints</b> check box.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Template</b>          | The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Set Type</b>          | The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Security Code</b>     | The security code for authorized access to the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Port</b>              | <p>The relevant port for the set type you select. You must select the port.</p> <p>The field lists the possible ports based on the selected set type.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Voice Mail Number</b> | <p>The voice mail number of the endpoint you associate with.</p> <p> <b>Note:</b></p> <p>You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of <b>Voice Mail Number</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Preferred Handle</b>  | <p>Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user.</p> <p>The <b>Preferred Handle</b> field is optional. Select numeric handle for alphanumeric support. By default, the field is blank.</p> <p>If the type of SIP entity is Communication Manager, Session Manager uses the preferred handle in the CM Endpoint profile. By default, for a SIP station, Communication Manager uses the extension number as the phone number entry on an OPS station-mapping table. If your enterprise dial plan has SIP handles that are different from the Communication Manager extension, then use the <b>Preferred Handle</b> field to change the phone number entry on the OPS station-mapping table on the Communication Manager.</p> <p>To modify the phone number entry, the Communication Address in System Manager should have a SIP handle. In the CM Endpoint Communication Profile, set the <b>Preferred Handle</b> field to the SIP handle format. After you click <b>Commit</b>, System Manager sets the <b>Phone Number</b> field in the OPS station-mapping table on Communication Manager to the SIP handle format. If you do not need this feature, then set the <b>Preferred Handle</b> value to <b>None</b>.</p> |
| <b>SIP URI</b>           | A unique alphanumeric communication address of the user to make and receive voice or video calls. The <b>SIP URI</b> address can be: <username-projectname>@<xyz.com>.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Attendant</b>         | <p>The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.</p> <p>When you select the 9641SIP template type from <b>Template</b>, the system enables the <b>Attendant</b> check box.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table continues...

| Name/Button                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enhanced Callr-Info display for 1-line phones</b>                       | <p>The option to activate the enhanced Callr-info operation on the phone.</p> <p>The <b>Enhanced Callr-Info display for 1-line phones</b> field on the station form is valid for the following set types:</p> <ul style="list-style-type: none"> <li>• 1603, 1608, 1616, 1408, 1416</li> <li>• 2402, 2410, 2420</li> <li>• 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625,</li> <li>• 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1</li> <li>• 7506D, 7507D</li> <li>• 8405D+, 8410D, 8405D, 8411D</li> <li>• 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650</li> </ul> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>No</b>: Does not change the callr-info interactions with the connected phone. The default setting.</li> <li>• <b>Yes</b>: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call, and on-call-release. If the <b>callr-info</b> button is not assigned to the phone on the station form, <b>Enhanced Callr-Info display for 1-line phones</b> does not apply.</li> </ul> |
| <b>Delete Endpoint on Unassign of Endpoint from User or on Delete User</b> | <p>The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or delete the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Override Endpoint Name and Localized Name</b>                           | <p>The option to override the following endpoint names:</p> <ul style="list-style-type: none"> <li>• The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization.</li> </ul> <p>If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization.</p> <ul style="list-style-type: none"> <li>• The localized display name on the Manage Users page in the <b>Localized Display Name</b> field of Communication Manager. If you clear the check box, the system does not override the localized display name in the <b>Localized Display Name</b> field.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Communication Profile tab - CS1000 Endpoint Profile

| Field         | Description                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------|
| <b>System</b> | The system that will be the element manager of the CS 1000 endpoint profile. You must select the system. |

*Table continues...*

| Field                                 | Description                                                                                                                                                                                                      |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b>                         | The system customer number of the CS 1000 system. You must select the target.<br>The system displays the field only when you select <b>Add new</b> .                                                             |
| <b>Template</b>                       | The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template.<br>The system displays the field only when you select <b>Add new</b> . |
| <b>Update</b>                         | The station profile information updated for the user. When you click <b>Update</b> , the system takes you to the element manager cut-through for the updates.                                                    |
| <b>Service Details</b>                | The service details of endpoints, such as set type, after phone creation.                                                                                                                                        |
| <b>Primary DN</b>                     | The primary directory number of the phone. You can enter only numeric values in this field.<br>The system displays the field only when you select <b>Add new</b> .                                               |
| <b>Include in Corporate Directory</b> | The option to add this profile to the CS 1000 Corporate Directory feature.                                                                                                                                       |

### Communication Profile tab — Messaging Profile

 **Note:**

The system displays the following fields only if you can configure a messaging profile for the user

| Name                                     | Description                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                            | The messaging system on which you add the subscriber. You must select the system.                                                                                                                                                                                                                                |
| <b>Use Existing Subscriber on System</b> | The option to specify whether to use an existing subscriber mailbox number to associate with this profile.                                                                                                                                                                                                       |
| <b>Mailbox Number</b>                    | The mailbox number of the subscriber. You must select the mailbox number.<br>The field takes the existing mailbox number that you associate with this profile. The value in the field is valid only if you select the <b>Use Existing Subscriber on System</b> check box.                                        |
| <b>Messaging Editor</b>                  | The Messaging application where you can edit or view details of the profile of the messaging endpoint.<br>After you save the changes in the Messaging system, the system does not update the modified data on the device or database until you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Template</b>                          | The system-defined or user-defined template that you associate with the subscriber.                                                                                                                                                                                                                              |
| <b>Password</b>                          | The password for logging in to the mailbox. You must provide the password.                                                                                                                                                                                                                                       |

*Table continues...*



| Name                                                                           | Description                                                                                                                                                                            |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Delete Subscriber on Unassign of Subscriber from User or on Delete User</b> | The option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this Messaging profile or delete the user. |

### Communication Profile tab: Avaya Messaging Profile

| Name                                     | Description                                                                                                                                                                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Officelinx System</b>                 | The Avaya Messaging system to which you add a mailbox.                                                                                                                                                                                                                |
| <b>Refresh</b>                           | The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use.<br><br>You do not require to refresh for every user.                                                             |
| <b>Mailbox Number</b>                    | The mailbox number of the subscriber.                                                                                                                                                                                                                                 |
| <b>Numeric Password</b>                  | The numeric password that is used to log in to the Avaya Messaging system.                                                                                                                                                                                            |
| <b>Confirm Numeric Password</b>          | The numeric password that you retype to confirm.                                                                                                                                                                                                                      |
| <b>Application User Password</b>         | The password that is used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.                                                                                                                       |
| <b>Confirm Application User Password</b> | The password that you retype to confirm.                                                                                                                                                                                                                              |
| <b>Company</b>                           | The name of the company to which the user belongs.                                                                                                                                                                                                                    |
| <b>Department</b>                        | The department to which the user belongs.                                                                                                                                                                                                                             |
| <b>Feature Group</b>                     | The feature group name that determines the rules for the mailboxes associated with it.                                                                                                                                                                                |
| <b>Capability</b>                        | The type of functionality that the user contains. The values are: <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Fax</b></li> <li>• <b>Messaging</b></li> <li>• <b>Collaboration</b></li> <li>• <b>Messaging and Collaboration</b></li> </ul> |
| <b>Domain Account Name</b>               | The mailbox NT account name of the Avaya Messaging profile.                                                                                                                                                                                                           |
| <b>Synchronization User Name</b>         | The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.                                                                                                                                                   |

 **Note:**

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

## Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

### \* Note:

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

| Name/Button                            | Description                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                          | The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.                                                                                                                                                                           |
| <b>Template</b>                        | The list of user templates from which you can select your preferred template to set the user configurations.                                                                                                                                                                                                                |
| <b>Use Existing Extension</b>          | Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.                                                                                                                                                   |
| <b>Extension</b>                       | The extension of the endpoint you associate with. You must select the extension.<br><br>The field lists the endpoints, existing or available, based on the option you selected in the <b>Use Existing Endpoints</b> check box.                                                                                              |
| <b>Endpoint Editor</b> button          | The option to start the IP Office application, where you can edit or view the details of the IP Office endpoint.<br><br>After you save the changes in IP Office manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Module-Port</b>                     | The module port combination list for IP Office analog extensions. You must select <b>Module-Port</b> for centralized users with Set Type as <b>Analog</b> .                                                                                                                                                                 |
| <b>Set Type</b>                        | The set type for the IP Office endpoint profile. By default, the <b>Set Type</b> field is disabled. If you select a template, the system populates the set type.                                                                                                                                                            |
| <b>Delete Extension On User Delete</b> | The option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with <b>Analog</b> and <b>Digital</b> set types.                                                                                   |

## Communication Profile tab: Equinox Conferencing

| Name                         | Description                                  |
|------------------------------|----------------------------------------------|
| <b>Equinox User Password</b> | The Equinox user password.                   |
| <b>Virtual Room Number</b>   | The virtual room number of the Equinox user. |

## Communication Profile tab — Presence Profile

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                              | <p>The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile:</p> <ul style="list-style-type: none"> <li>• Aggregate presence</li> <li>• Archive instant messages if the Instant Messages option is enabled</li> </ul>            |
| <b>SIP Entity</b>                          | <p>The option to route the SIP-based messages through Presence Services. This system selects the SIP entity only if you select a Presence Services instance in the <b>System</b> field. <b>SIP Entity</b> is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.</p>                                                                      |
| <b>IM Gateway SIP Entity</b>               | The Presence Services instance for the user.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Publish Presence with AES Collector</b> | <p>The option that determines if Presence Services must publish presence with AES Collector. The options are:</p> <ul style="list-style-type: none"> <li>• <b>System Default</b></li> <li>• <b>Off</b></li> <li>• <b>On</b></li> </ul> <p>The default is <b>System Default</b>. You can change the default value. You do not require to configure AES Collector in the Presence Services server.</p> |

## Communication Profile tab: Conferencing Profile

| Name                                                         | Description                                                                                                                                                                                                                                          |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Auto-generated Code Length</b>                     | <p>The number of characters in PIN. The default is 6.</p> <p>The system displays this field if you select the <b>Auto Generate Participant and Moderator Security Code</b> check box.</p>                                                            |
| <b>Auto Generate Participant and Moderator Security Code</b> | <p>Select the check box if the system must generate the participant security code and moderator security code for this user.</p> <p>Clear the check box to assign a specific participant security code or moderator security code for this user.</p> |
| <b>Participant Security Code</b>                             | <p>The participant security code that you assign for this user.</p> <p>The system displays this field only when the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.</p>                                             |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Moderator Security Code</b> | The moderator security code that you assign for this user.<br><br>The system displays this field if the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.                                                                       |
| <b>Location</b>                | The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.<br><br>For SIP users, the system uses the location value from the <b>Home Location</b> field in the Session Manager profile. |
| <b>Template</b>                | The Conferencing template that you assign to this user.                                                                                                                                                                                                        |

| Button               | Description                                                                     |
|----------------------|---------------------------------------------------------------------------------|
| <b>Get Templates</b> | Displays the list of Conferencing templates, which you can assign to this user. |

### Communication Profile tab: Work Assignment Profile

| Name                   | Description          |
|------------------------|----------------------|
| <b>Account</b>         | The account name.    |
| <b>Account Address</b> | The account address. |
| <b>Source</b>          | The source name.     |
| <b>Source Address</b>  | The source address.  |

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

| Button                  | Description                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Resource Details</b> | Displays the Assignment Management page where you can configure assignment targets for the user.<br><br>You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user. |
| <b>Account Details</b>  | Displays the text box where you can add or modify the account name and account address.<br><br>You can add attributes to the account only when the account is added to the agent.                                            |
| <b>Source Details</b>   | Displays the text box where you can add or modify the source name and source address.<br><br>You can add properties and attributes to the source only when the source already exists.                                        |

**Membership tab — Roles**

| Name             | Description                                                                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select check box | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| Name             | The name of the role.                                                                                                                                        |
| Description      | A brief description about the role.                                                                                                                          |

| Button         | Description                                                                             |
|----------------|-----------------------------------------------------------------------------------------|
| Assign Roles   | Displays the Assign Role page that you can use to assign the roles to the user account. |
| Unassign Roles | Removes the selected role from the list of roles associated with the user account.      |

**Membership tab — Group Membership**

| Name             | Description                                 |
|------------------|---------------------------------------------|
| Select check box | Use this check box to select a group.       |
| Name             | The name of the group.                      |
| Type             | The group type based on the resources.      |
| Hierarchy        | The position of the group in the hierarchy. |
| Description      | A brief description about the group.        |

| Button            | Description                                                                  |
|-------------------|------------------------------------------------------------------------------|
| Add To group      | Displays the Assign Groups page that you can use to add the user to a group. |
| Remove From Group | Removes the user from the selected group.                                    |

**Contacts tab — Default Contact List**

| Name        | Description                              |
|-------------|------------------------------------------|
| Description | A brief description of the contact list. |

**Contacts tab — Associated Contacts**

| Name             | Description                                                                                    |
|------------------|------------------------------------------------------------------------------------------------|
| Last Name        | The last name of the contact.                                                                  |
| First Name       | The first name of the contact.                                                                 |
| Scope            | The categorization of the contact based on whether the contact is a public or private contact. |
| Speed Dial       | The value specifies whether the speed dial is set for the contact or not.                      |
| Speed Dial Entry | The reduced number that represents the speed dial number.                                      |

*Table continues...*

| Name                  | Description                                                                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Presence Buddy</b> | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you cannot track the presence of the contact. |

| Button             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>        | Displays the Edit Contact List Member page. Use this page to modify the information of the selected contact.                                                                                                                                                                                                                                                                                                                                       |
| <b>Add</b>         | <p>Displays the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.</p> <p>In the Multi Tenancy environment, when the tenant administrator of a tenant creates or updates the user, the administrator can attach only the following contacts:</p> <ul style="list-style-type: none"> <li>• Private contacts of the user</li> <li>• Public contacts</li> <li>• Users who belong to that tenant</li> </ul> |
| <b>Remove</b>      | Removes one or more selected contacts from the list of the associated contacts.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Filter menu</b> | <p>You can find the <b>Filter menu</b> icon next to the name of each column.</p> <p>Filters the data based on the search criteria.</p>                                                                                                                                                                                                                                                                                                             |

## Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                              |
|------------------------|------------------------------------------|
| <b>Last Name</b>       | The last name of the private contact.    |
| <b>First Name</b>      | The first name of the contact.           |
| <b>Display Name</b>    | The display name of the private contact. |
| <b>Contact Address</b> | The address of the private contact.      |
| <b>Description</b>     | A brief description about the contact.   |

| Button             | Description                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>        | Displays the Edit Private Contact page. Use this page to edit the information of the contact you selected.                             |
| <b>New</b>         | Displays the <b>New Private Contact</b> page. Use this page to add a new private contact.                                              |
| <b>Delete</b>      | Deletes the selected contacts.                                                                                                         |
| <b>Filter menu</b> | <p>You can find the <b>Filter menu</b> icon next to the name of each column.</p> <p>Filters the data based on the search criteria.</p> |

## Common buttons

| Button                       | Description                                                                                                                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commit &amp; Continue</b> | Saves your changes and retains you on the same page for further modifications.                                                                                                                                                                                                                                                   |
| <b>Commit</b>                | <p>Modifies the user account and takes you back to the User Management or User Profile   View   &lt;User Name&gt; page.</p> <p> <b>Note:</b></p> <p>While restoring a deleted user, use the <b>Commit</b> button to restore a deleted user.</p> |
| <b>Cancel</b>                | Cancels the operation of modifying the user information and takes you back to the User Management or User Profile   View   <User Name> page.                                                                                                                                                                                     |

## User Profile | View | <User Name> field descriptions

### Organization

| Name           | Description                                                                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tenant</b>  | The name of the tenant that you select.                                                                                                                                       |
| <b>Level 1</b> | <p>The name of the level 1 hierarchy of the tenant organization. For example, Site.</p> <p>The tenant administrator provides the hierarchy on the Tenant Management page.</p> |
| <b>Level 2</b> | The name of the level 2 hierarchy of the tenant organization. For example, Department.                                                                                        |
| <b>Level 3</b> | The name of the level 3 hierarchy of the tenant organization. For example, Team.                                                                                              |

### User Provisioning Rule

| Name                          | Description                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>User Provisioning Rule</b> | <p>The name of the user provisioning rule.</p> <p>You can provide only one user provisioning rule.</p> |

 **Note:**

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

**Identity tab — Identity section**

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>                      | The last name of the user. For example, Miller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p> <b>Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>• Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>• Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the user. For example, John.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Middle Name</b>                    | The middle name of the user, if any.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>                    | A brief description of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Status</b>                         | The login status of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Update Time</b>                    | The time when the user details were last modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Login Name</b>                     | <p>The unique system login name given to the user. The login name takes the form of username@domain. You use the login name to create the user's primary handle.</p> <p>The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter the login name in uppercase or lowercase.</p> <p>You cannot edit the <b>Login Name</b> field for users with the login name admin.</p>                                                                                                                                                                                                                             |
| <b>Email Address</b>                  | The email address of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

*Table continues...*



| Name                          | Description                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Type</b>    | Authentication type defines how the system performs user authentication. The options are: <ul style="list-style-type: none"> <li>• <b>Enterprise:</b> The enterprise authenticates the user login.</li> <li>• <b>Basic:</b> Avaya Authentication Service authenticates the user login.</li> </ul> |
| <b>Source</b>                 | The entity that created this user record. The options are IP Address/Port, or a name representing an enterprise LDAP, or Avaya.                                                                                                                                                                   |
| <b>Localized Display Name</b> | The localized display name of a user. Usually, the name is the localized full name.                                                                                                                                                                                                               |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. The field supports display names that cannot handle localized text, for example, some endpoints.                                                                                                                                             |
| <b>Title</b>                  | The personal title for address a user. Usually, the title is a social title and not the work title.                                                                                                                                                                                               |
| <b>Language Preference</b>    | The preferred written or spoken language of the user.                                                                                                                                                                                                                                             |
| <b>Time Zone</b>              | The preferred time zone of the user.                                                                                                                                                                                                                                                              |
| <b>Employee ID</b>            | The employee number for the user.                                                                                                                                                                                                                                                                 |
| <b>Department</b>             | The department to which the user belongs.                                                                                                                                                                                                                                                         |
| <b>Company</b>                | The organization where the user works.                                                                                                                                                                                                                                                            |

### Identity tab — Address section

| Name                | Description                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>         | The unique label that identifies the address.                                                                               |
| <b>Address Type</b> | The type of the address. Types of addresses are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>       | The name of the street.                                                                                                     |
| <b>City</b>         | The name of the city or town.                                                                                               |
| <b>Postal Code</b>  | The postal code used by postal services to route mail to a destination. In United States, this is Zip code.                 |
| <b>Province</b>     | The full name of the province.                                                                                              |
| <b>Country</b>      | The name of the country.                                                                                                    |

**Identity tab — Localized Names section**

| Name         | Description                                           |
|--------------|-------------------------------------------------------|
| Language     | The localized languages for displaying the user name. |
| Display Name | The user name in the localized language you choose.   |

| Button | Description                                          |
|--------|------------------------------------------------------|
| New    | Allows you to add a new localized name for the user. |
| Edit   | Allows you to edit the localized name for the user.  |
| Delete | Deletes the localized names you select for the user. |
| Add    | Adds or edits the localized name for the user.       |
| Cancel | Cancels your add or edit of the localized name.      |

**Communication Profile tab — Communication Profile**

Use this section to create, modify, and delete a communication profile of the user. Each communication profile can contain one or more communication addresses for a user.

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Communication Profile Password | <p>The communication profile password.</p> <p>The field is available only if you enable the communication profile. The password policy is configured on the <b>Users &gt; User Management &gt; Communication Profile Password Policy</b> page.</p> <p>When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user.</p> <p>For information about password policy, see “Communication profile password policy”.</p> |

*Table continues...*

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generate</b> | <p>The option to automatically generate the communication profile password.</p> <p>System Manager sends the generated password to the user if you:</p> <ul style="list-style-type: none"> <li>Set the email configuration properties on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR</b> page.</li> </ul> <p>For more information, see “Configuring email properties”.</p> <ul style="list-style-type: none"> <li>Configure <b>Email Address</b> on the <b>Identity</b> tab.</li> </ul> <p>By default, the <b>Generate</b> link is available for creating a new user account.</p> <p>The <b>Edit</b> link is available for modifying user accounts. When you click the <b>Edit</b> link, the system displays <b>Confirm Password</b> along with the <b>Generate</b> and <b>Cancel</b> links.</p> |
| <b>Name</b>     | The name of the communication profile that you must select .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.                                          |
| <b>Done</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancels the operation of adding a communication profile.                             |

The system enables the following fields when you click **New** in the Communication Profile section.

### Communication Profile tab — Communication Address section

| Name          | Description                                                 |
|---------------|-------------------------------------------------------------|
| <b>Type</b>   | The type of the handle.                                     |
| <b>Handle</b> | The unique communication address for the user.              |
| <b>Domain</b> | The name of the domain with which the handle is registered. |

### Communication Profile tab — Session Manager section

#### **Note:**

The system displays the following fields only if a communication profile of the user exists for the product:

| Name                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Session Manager</b>                                  | The Session Manager instance that you use as home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point to connect devices that are associated with the communication profile to the Avaya network. A selection is required.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Secondary Session Manager</b>                                | If you select a secondary Session Manager instance, this Session Manager provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager becomes unavailable. A selection is optional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Survivability Server</b>                                     | <p>For local survivability, a survivability server that you can specify to provide survivability communication services for devices associated with a communication profile if local connectivity to Session Manager instances in Avaya Aura® is lost. If Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.</p> <p> <b>Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, the Communication Manager associated with the application must be the main Communication Manager for the Communication Manager survivable remote server that is resident with Branch Session Manager.</p> |
| <b>Max. Simultaneous Devices</b>                                | The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Block New Registration When Maximum Registrations Active</b> | If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Origination Application Sequence</b> | <p>An application sequence that will be invoked when the system routes the calls from this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> |
| <b>Termination Application Sequence</b> | <p>An application sequence that will be invoked when calls are routed to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p>              |
| <b>Conference Factory Set</b>           | <p>The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.</p> <p>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.</p>                                                                                                                                                                           |
| <b>Home Location</b>                    | <p>The location that Session Manager uses when the IP address of the calling phone does not match any IP address pattern of any location. This field is specified to support mobility of the user.</p>                                                                                                                                                                                                                                        |

### Communication Profile tab: Avaya Breeze® platform Profile

| Name                   | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Service Profile</b> | The profile that you assign to the user. The user can gain access to the service contained in the profile. |

### Communication Profile tab — CM Endpoint Profile

 **Note:**

The system displays these fields only if a Communication Manager Endpoint profile exists for the user.

| Name/Button              | Description                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>            | Communication Manager on which you add the endpoint.<br><br>The Communication Manager system on which you add the endpoint. You must select the system.                                                                                                                                                                                                |
| <b>Profile Type</b>      | The type of the profile for the user.                                                                                                                                                                                                                                                                                                                  |
| <b>Extension</b>         | The extension of the endpoint that you associate this profile with. You must select the extension.                                                                                                                                                                                                                                                     |
| <b>View Endpoint</b>     | The list of existing or available endpoints based on the selection of the <b>Use Existing Endpoints</b> check box.                                                                                                                                                                                                                                     |
| <b>Set Type</b>          | The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.                                                                                                                                                                                                                         |
| <b>Security Code</b>     | The security code for authorized access to the endpoint.                                                                                                                                                                                                                                                                                               |
| <b>Port</b>              | The relevant port for the set type you select. You must select the port.                                                                                                                                                                                                                                                                               |
| <b>Voice Mail Number</b> | The voice mail number of the endpoint you associate with.<br><br> <b>Note:</b><br><br>You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of <b>Voice Mail Number</b> .                                           |
| <b>Preferred Handle</b>  | Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user.<br><br>The <b>Preferred Handle</b> field is optional. Select numeric handle for alphanumeric support. By default, the field is blank.<br><br>If SIP entity is of the Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile. |
| <b>SIP URI</b>           | A unique alphanumeric communication address of the user to make and receive voice or video calls. The <b>SIP URI</b> address can be: <username-projectname>@<xyz.com>.                                                                                                                                                                                 |
| <b>Attendant</b>         | The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.<br><br>When you select the 9641SIP template type from <b>Template</b> , the system enables the <b>Attendant</b> check box.                                                                                  |

*Table continues...*

| Name/Button                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enhanced Callr-Info display for 1-line phones</b>                    | <p>The option to activate the enhanced Callr-info operation on the phone.</p> <p>The <b>Enhanced Callr-Info display for 1-line phones</b> field on the station form is valid for the following set types:</p> <ul style="list-style-type: none"> <li>• 1603, 1608, 1616, 1408, 1416</li> <li>• 2402, 2410, 2420</li> <li>• 4606, 4612, 4612CL, 4624, 4602, 4602+, 4630, 4610, 4622, 4620, 4621, 4625,</li> <li>• 6402D, 6408D, 6408D+, 6416D+, 6424D+, 607A1</li> <li>• 7506D, 7507D</li> <li>• 8405D+, 8410D, 8405D, 8411D</li> <li>• 9404, 9408, 9601, 9601+, 9610, 9620, 9621, 9608, 9611, 9630, 9640, 9641, 9650</li> </ul> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>No</b>: Does not change the callr-info interactions with the connected phone. The default setting.</li> <li>• <b>Yes</b>: Activates the enhanced Callr-info operation including the application of the existing feature related system parameters. Clear Callr-Info option settings of leave-ACW, next-call, and on-call-release. If the <b>callr-info</b> button is not assigned to the phone on the station form, <b>Enhanced Callr-Info display for 1-line phones</b> does not apply.</li> </ul> |
| <b>Delete Endpoint on Unassign of Endpoint from User or Delete User</b> | <p>The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or delete the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Override Endpoint Name</b>                                           | <p>The option to override the following:</p> <ul style="list-style-type: none"> <li>• The endpoint name on Communication Manager with the value you configured on the Manage users page during synchronization.</li> </ul> <p>If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization.</p> <ul style="list-style-type: none"> <li>• The localized display name on the Manage Users page in the <b>Localized Display Name</b> field of Communication Manager. If you clear the check box, the system does not override the localized display name in the <b>Localized Display Name</b> field.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Communication Profile tab - CS1000 Endpoint Profile**

| Name                                  | Description                                                                                                                                                                   |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                         | The CS 1000 system of the endpoint.                                                                                                                                           |
| <b>Target</b>                         | The system customer number for the Communication Server.                                                                                                                      |
| <b>Template</b>                       | The phone or endpoint template that you can choose for the user. The element manager maintains all templates.                                                                 |
| <b>Update</b>                         | The option to update the endpoint profile information for the user. When you click <b>Update</b> , the system takes displays the element manager cut through for the updates. |
| <b>Service Details</b>                | The service details, such as set type of endpoints that the system displays after phone creation.                                                                             |
| <b>Primary DN</b>                     | The primary directory number of the phone. You can enter only numeric values.                                                                                                 |
| <b>Include in Corporate Directory</b> | The option to add this profile to the CS 1000 corporate directory.                                                                                                            |

**Communication Profile tab — Messaging Profile****\* Note:**

The system displays the following fields only if you can configure a messaging profile for the user

| Name                                                         | Description                                                                                                                                                                                              |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                                | The messaging system on which you add the subscriber.                                                                                                                                                    |
| <b>Template</b>                                              | The template, system-defined or user-defined, that you associate with the subscriber.                                                                                                                    |
| <b>Mailbox Number</b>                                        | The mailbox number of the subscriber.                                                                                                                                                                    |
| <b>Password</b>                                              | The password for logging on to the mailbox.                                                                                                                                                              |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Provides the option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this messaging profile or when you delete the user. |

**Communication Profile tab: Avaya Messaging Profile**

| Name                     | Description                                            |
|--------------------------|--------------------------------------------------------|
| <b>Officelinx System</b> | The Avaya Messaging system to which you add a mailbox. |

*Table continues...*



| Name                                     | Description                                                                                                                                                                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Refresh</b>                           | The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use.<br><br>You do not require to refresh for every user.                                                             |
| <b>Mailbox Number</b>                    | The mailbox number of the subscriber.                                                                                                                                                                                                                                 |
| <b>Numeric Password</b>                  | The numeric password that is used to log in to the Avaya Messaging system.                                                                                                                                                                                            |
| <b>Confirm Numeric Password</b>          | The numeric password that you retype to confirm.                                                                                                                                                                                                                      |
| <b>Application User Password</b>         | The password that is used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.                                                                                                                       |
| <b>Confirm Application User Password</b> | The password that you retype to confirm.                                                                                                                                                                                                                              |
| <b>Company</b>                           | The name of the company to which the user belongs.                                                                                                                                                                                                                    |
| <b>Department</b>                        | The department to which the user belongs.                                                                                                                                                                                                                             |
| <b>Feature Group</b>                     | The feature group name that determines the rules for the mailboxes associated with it.                                                                                                                                                                                |
| <b>Capability</b>                        | The type of functionality that the user contains. The values are: <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Fax</b></li> <li>• <b>Messaging</b></li> <li>• <b>Collaboration</b></li> <li>• <b>Messaging and Collaboration</b></li> </ul> |
| <b>Domain Account Name</b>               | The mailbox NT account name of the Avaya Messaging profile.                                                                                                                                                                                                           |
| <b>Synchronization User Name</b>         | The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.                                                                                                                                                   |

 **Note:**

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

### Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

 **Note:**

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

| Name/Button                                      | Description                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                    | The list of IP Office device names from which you can select the IP Office device you associate with the user.                                                                                                                                                                                                 |
| <b>Template</b>                                  | The list of user templates from which you can select your preferred template to set the user configurations.                                                                                                                                                                                                   |
| <b>Use Existing Extension</b>                    | Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.                                                                                                                                      |
| <b>Extension</b>                                 | The extension of the endpoint you associate.<br><br>The field lists the endpoints, existing or available, based on option you selected in the <b>Use Existing Endpoints</b> check box.                                                                                                                         |
| <b>Endpoint Editor</b> button                    | Starts the IP Office application, where you can edit or view the details of the IP Office endpoint.<br><br>After you save the changes in IP Office manager, the system does not update the modified data on the device or database until you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Module-Port</b>                               | The module port combination list for IP Office analog extensions. You must select <b>Module-Port</b> for centralized users with Set Type as <b>Analog</b> .                                                                                                                                                    |
| <b>Set Type</b>                                  | The set type for the IP Office endpoint profile. By default, the <b>Set Type</b> field is disabled. If you select a template, the set type is auto populated.                                                                                                                                                  |
| <b>Delete Extension On User Delete</b> check box | Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with <b>Analog</b> and <b>Digital</b> set types.                                                             |

## Communication Profile tab: Equinox Conferencing

| Name                         | Description                                  |
|------------------------------|----------------------------------------------|
| <b>Equinox User Password</b> | The Equinox user password.                   |
| <b>Virtual Room Number</b>   | The virtual room number of the Equinox user. |

## Communication Profile tab — Presence Profile

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                              | <p>The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile:</p> <ul style="list-style-type: none"> <li>• Aggregate presence</li> <li>• Archive instant messages if the Instant Messages option is enabled</li> </ul>            |
| <b>SIP Entity</b>                          | <p>The option to route the SIP-based messages through Presence Services. This system selects the SIP entity only if you select a Presence Services instance in the <b>System</b> field. <b>SIP Entity</b> is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.</p>                                                                      |
| <b>IM Gateway SIP Entity</b>               | The Presence Services instance for the user.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Publish Presence with AES Collector</b> | <p>The option that determines if Presence Services must publish presence with AES Collector. The options are:</p> <ul style="list-style-type: none"> <li>• <b>System Default</b></li> <li>• <b>Off</b></li> <li>• <b>On</b></li> </ul> <p>The default is <b>System Default</b>. You can change the default value. You do not require to configure AES Collector in the Presence Services server.</p> |

## Communication Profile tab: Conferencing Profile

| Name                                                         | Description                                                                                                                                                                                                                                          |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Auto-generated Code Length</b>                     | <p>The number of characters in PIN. The default is 6.</p> <p>The system displays this field if you select the <b>Auto Generate Participant and Moderator Security Code</b> check box.</p>                                                            |
| <b>Auto Generate Participant and Moderator Security Code</b> | <p>Select the check box if the system must generate the participant security code and moderator security code for this user.</p> <p>Clear the check box to assign a specific participant security code or moderator security code for this user.</p> |
| <b>Participant Security Code</b>                             | <p>The participant security code that you assign for this user.</p> <p>The system displays this field only when the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.</p>                                             |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Moderator Security Code</b> | The moderator security code that you assign for this user.<br><br>The system displays this field if the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.                                                                       |
| <b>Location</b>                | The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.<br><br>For SIP users, the system uses the location value from the <b>Home Location</b> field in the Session Manager profile. |
| <b>Template</b>                | The Conferencing template that you assign to this user.                                                                                                                                                                                                        |

| Button               | Description                                                                     |
|----------------------|---------------------------------------------------------------------------------|
| <b>Get Templates</b> | Displays the list of Conferencing templates, which you can assign to this user. |

### Communication Profile tab: Work Assignment Profile

| Name                   | Description          |
|------------------------|----------------------|
| <b>Account</b>         | The account name.    |
| <b>Account Address</b> | The account address. |
| <b>Source</b>          | The source name.     |
| <b>Source Address</b>  | The source address.  |

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

| Button                  | Description                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Resource Details</b> | Displays the Assignment Management page where you can configure assignment targets for the user.<br><br>You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user. |
| <b>Account Details</b>  | Displays the text box where you can add or modify the account name and account address.<br><br>You can add attributes to the account only when the account is added to the agent.                                            |
| <b>Source Details</b>   | Displays the text box where you can add or modify the source name and source address.<br><br>You can add properties and attributes to the source only when the source already exists.                                        |

### Membership tab — Roles section

| Name        | Description           |
|-------------|-----------------------|
| <b>Name</b> | The name of the role. |

*Table continues...*

| Name        | Description                         |
|-------------|-------------------------------------|
| Description | A brief description about the role. |

### Membership tab — Group Membership section

| Name        | Description                                 |
|-------------|---------------------------------------------|
| Name        | The name of the group.                      |
| Type        | The group type based on the resources.      |
| Hierarchy   | The position of the group in the hierarchy. |
| Description | A brief description about the group.        |

### Contacts tab — Default Contact List section

| Name        | Description                              |
|-------------|------------------------------------------|
| Description | A brief description of the contact list. |

### Contacts tab — Associated Contacts section

| Name             | Description                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Last Name        | The last name of the contact.                                                                                                                                                 |
| First Name       | The first name of the contact.                                                                                                                                                |
| Scope            | The categorization of the contact based on whether the contact is a public or private contact.                                                                                |
| Speed Dial       | The value that specifies whether the speed dial is set for the contact.                                                                                                       |
| Speed Dial Entry | The reduced number that represents the speed dial number.                                                                                                                     |
| Presence Buddy   | The value that specifies whether you can monitor the presence information of the contact or not.<br><b>False</b> indicates that you cannot track the presence of the contact. |

| Button      | Description                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| Filter menu | You can find the <b>Filter menu</b> icon next to the name of each column.<br><br>Filters the data based on the search criteria. |

### Contacts tab — Private Contacts section

Use this section to add new private contacts, modify and deletes existing contacts.

| Name       | Description                            |
|------------|----------------------------------------|
| Last Name  | The last name of the private contact.  |
| First Name | The first name of the private contact. |

*Table continues...*

| Name                   | Description                            |
|------------------------|----------------------------------------|
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | The address of the private contact.    |
| <b>Description</b>     | A brief description about the contact. |

| Button             | Description                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter menu</b> | You can find the <b>Filter menu</b> icon next to the name of each column.<br><br>Filters the data based on the search criteria. |

### Common buttons

| Button      | Description                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the User Profile   Edit   <User Name> page. Use the User Profile   Edit   <User Name> page to modify the details of the user account. |
| <b>Done</b> | Closes the User Profile   Edit   <User Name> page and returns to the User Management page.                                                     |

## User Profile | Duplicate | <User Name> field descriptions

### Organization

| Name           | Description                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tenant</b>  | The name of the tenant that you select.                                                                                                                                |
| <b>Level 1</b> | The name of the level 1 hierarchy of the tenant organization. For example, Site.<br><br>The tenant administrator provides the hierarchy on the Tenant Management page. |
| <b>Level 2</b> | The name of the level 2 hierarchy of the tenant organization. For example, Department.                                                                                 |
| <b>Level 3</b> | The name of the level 3 hierarchy of the tenant organization. For example, Team.                                                                                       |

### User Provisioning Rule

| Name                          | Description                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------|
| <b>User Provisioning Rule</b> | The name of the user provisioning rule.<br><br>You can provide only one user provisioning rule. |

#### **Note:**

When you use the user provisioning rule to create a user, the system populates the values of user attributes from the user provisioning rule.

**\* Note:**

You cannot edit the tenant. If you select a different level 1 for the tenant from the organization hierarchy, the **Level 2** and **Level 3** fields become blank. You can select new values for level 2 and level 3. If you select a different level 2 for the tenant from the organization hierarchy, the **Level 3** field becomes blank. You can select a new value for level 3.

## Identity tab — Identity section

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>                      | The last name of the user. For example, Miller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p><b>* Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the user. For example, John.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Middle Name</b>                    | The middle name of the user, if any.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>                    | A brief description of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Login Name</b>                     | <p>The unique system login name given to the user. The login name takes the form of username@domain. You use the login name to create the primary handle of the user.</p> <p>The login name is not case-sensitive. For example, if you enter JMILLER@AVAYA.COM, the system converts the login name to lowercase, that is, jmiller@avaya.com. However, on the login page, you can enter the login name in uppercase or lowercase.</p> <p>You cannot edit the <b>Login Name</b> field for users with the login name admin.</p>                                                                                                                                    |
| <b>Email Address</b>                  | The email address of the user for receiving email notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Type</b>              | Authentication type defines how the system performs user's authentication. The options are: <ul style="list-style-type: none"> <li>• <b>Enterprise:</b> User's login is authenticated by the enterprise.</li> <li>• <b>Basic:</b> User's login is authenticated by an Avaya Authentication Service.</li> </ul> |
| <b>Password</b>               | Type your password for the duplicate profile.                                                                                                                                                                                                                                                                  |
| <b>Confirm Password</b>       | Retype your password for confirmation.                                                                                                                                                                                                                                                                         |
| <b>Localized Display Name</b> | The localized display name of a user. It is typically the localized full name.                                                                                                                                                                                                                                 |
| <b>Endpoint Display Name</b>  | The full text name of the user represented in ASCII. It supports displays that cannot handle localized text, for example, some endpoints.                                                                                                                                                                      |
| <b>Title</b>                  | The personal title for address a user. This is typically a social title and not the work title.                                                                                                                                                                                                                |
| <b>Language Preference</b>    | The user's preferred written or spoken language.                                                                                                                                                                                                                                                               |
| <b>Time Zone</b>              | The preferred time zone of the user.                                                                                                                                                                                                                                                                           |
| <b>Employee ID</b>            | The employee number for the user.                                                                                                                                                                                                                                                                              |
| <b>Department</b>             | The department which the user belongs to.                                                                                                                                                                                                                                                                      |
| <b>Company</b>                | The organization where the user works.                                                                                                                                                                                                                                                                         |

### Identity tab — Address section

| Name                | Description                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>check box</b>    | Use this check box to select the address.                                                                       |
| <b>Name</b>         | The unique label that identifies the address.                                                                   |
| <b>Address Type</b> | The type of address. The values are: <ul style="list-style-type: none"> <li>• Office</li> <li>• Home</li> </ul> |
| <b>Street</b>       | The name of the street.                                                                                         |
| <b>City</b>         | The name of the city or town.                                                                                   |
| <b>Postal Code</b>  | The postal code used by postal services to route mail to a destination. In United States this is Zip code.      |
| <b>Province</b>     | The full name of the province.                                                                                  |
| <b>Country</b>      | The name of the country.                                                                                        |

| Button      | Description                                                                    |
|-------------|--------------------------------------------------------------------------------|
| <b>New</b>  | Displays the Add Address page that you can use to add the address details.     |
| <b>Edit</b> | Displays the Edit Address page that you can use to modify the address details. |

*Table continues...*



| Button                       | Description                                                                   |
|------------------------------|-------------------------------------------------------------------------------|
| <b>Delete</b>                | Deletes the selected address.                                                 |
| <b>Choose Shared Address</b> | Displays the Choose Address page that you can use to choose a common address. |

### Identity tab — Localized Names section

| Name                | Description                                           |
|---------------------|-------------------------------------------------------|
| <b>Language</b>     | The localized languages for displaying the user name. |
| <b>Display Name</b> | The user name in the localized language you choose.   |

| Button        | Description                                          |
|---------------|------------------------------------------------------|
| <b>New</b>    | Allows you to add a new localized name for the user. |
| <b>Edit</b>   | Allows you to edit the localized name for the user.  |
| <b>Delete</b> | Deletes the localized names you select for the user. |
| <b>Add</b>    | Adds or edits the localized name for the user.       |
| <b>Cancel</b> | Cancels your add or edit of the localized name.      |

| Button        | Description                                                                  |
|---------------|------------------------------------------------------------------------------|
| <b>Commit</b> | Creates the duplicate user.                                                  |
| <b>Cancel</b> | Cancels the duplicate user creation and returns to the User Management page. |

### Communication Profile tab — Communication Profile section

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Communication Profile Password</b> | <p>The communication profile password.</p> <p>The field is available only if you enable the communication profile. The password policy is configured on the <b>Users &gt; User Management &gt; Communication Profile Password Policy</b> page.</p> <p>When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user.</p> <p>For information about password policy, see “Communication profile password policy”.</p> |
| <b>Confirm Password</b>               | The communication profile password that you reenter for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generate</b> | <p>The option to automatically generate the communication profile password.</p> <p>System Manager sends the generated password to the user if you:</p> <ul style="list-style-type: none"> <li>Set the email configuration properties on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR</b> page.</li> </ul> <p>For more information, see “Configuring email properties”.</p> <ul style="list-style-type: none"> <li>Configure <b>Email Address</b> on the <b>Identity</b> tab.</li> </ul> <p>By default, the <b>Generate</b> link is available for creating a new user account.</p> <p>The <b>Edit</b> link is available for modifying user accounts. When you click the <b>Edit</b> link, the system displays <b>Confirm Password</b> along with the <b>Generate</b> and <b>Cancel</b> links.</p> |
| <b>Name</b>     | The name of the communication profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>New</b>    | Creates a new communication profile for the user.                                    |
| <b>Delete</b> | Deletes the selected communication profile.                                          |
| <b>Save</b>   | Saves the communication profile information that you updated or added for a profile. |
| <b>Cancel</b> | Cancels the operation for adding a communication profile.                            |

The page displays the following fields when you click the **New** button in the Communication Profile section.

| Name           | Description                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------|
| <b>Name</b>    | The name of the communication profile of the user.                                                      |
| <b>Default</b> | The profile that is made default is the active profile. There can be only one active profile at a time. |

### Communication Profile tab — Communication Address section

| Name          | Description                                          |
|---------------|------------------------------------------------------|
| <b>Type</b>   | The communication protocol to be used for the user.  |
| <b>Handle</b> | A unique communication address for the user.         |
| <b>Domain</b> | The domain name with which the handle is registered. |

| Button        | Description                                                   |
|---------------|---------------------------------------------------------------|
| <b>New</b>    | Displays the fields for adding a new communication address.   |
| <b>Edit</b>   | Saves the changes that you made to the communication address. |
| <b>Delete</b> | Deletes the selected communication address.                   |

The page displays the following fields when you click **New** and **Edit** in the Communication Address section.

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>                    | <p>The type of handle. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Avaya SIP</b>: Indicates that the handle supports Avaya SIP-based communication.</li> <li>• <b>Avaya E.164</b>: Indicates that the handle refers to an E.164 formatted address. E.164 numbers can have maximum 13 digits and are usually written with a + prefix.</li> <li>• <b>Microsoft SIP</b>: Indicates that the handle supports SIP-based communication.</li> <li>• <b>Microsoft Exchange</b>: Indicates that the handle is an email address and supports communication with Microsoft SMTP server.</li> <li>• <b>Lotus Notes</b>: Indicates that the handle is for Lotus Notes and domino calendar.</li> <li>• <b>IBM Sametime</b>: Indicates that the handle is for IBM Sametime. The address must be in the DN=IBMHandle format.</li> <li>• <b>Avaya Presence/IM</b>: Indicates that the handle is an address that is used for Extensible Messaging and Presence Protocol (XMPP)-based Internet Messaging (IM) services and XMPP or Session Initiation Protocol-based (SIP) Presence services.</li> </ul> <p> <b>Note:</b></p> <p>To create the Presence communication profile, you must select <b>Avaya Presence/IM</b> and provide the communication address.</p> <ul style="list-style-type: none"> <li>• <b>GoogleTalk</b>: Indicates that the handle supports XMPP-based communication with the Google Talk service.</li> <li>• <b>Other Email</b>: Indicates that the handle is an email address other than MS Exchange email addresses.</li> <li>• <b>Other SIP</b>: Indicates that the handle supports SIP-based communication other than the listed ones.</li> <li>• <b>Other XMPP</b>: Indicates that the handle supports XMPP-based communication other than the listed ones.</li> <li>• <b>Work Assignment</b>: Indicates that the handle supports accounts that can be assigned to an agent for Work Assignment.</li> </ul> |
| <b>Fully Qualified Address</b> | <p>The fully qualified domain name or uniform resource identifier. The address can be an email address, IM user, or an address of a communication device by using which the user can send or receive messages. You must provide the fully qualified address.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Button        | Description                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------|
| <b>Add</b>    | Saves the new communication address or modified communication address information in the database. |
| <b>Cancel</b> | Cancels the addition of communication address.                                                     |

### Communication Profile tab — Session Manager

**\* Note:**

The system displays the following fields only if a communication profile of the user exists for the product:

| Name                                    | Description                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Session Manager</b>          | Select the Session Manager instance that should be used as the home server for the currently displayed Communication Profile. As a home server, the selected primary Session Manager instance will be used as the default access point for connecting devices associated with the Communication Profile to the Aura network. A selection is required. |
| <b>Secondary Session Manager</b>        | The secondary Session Manager instance that provides continued service to SIP devices associated with this Communication Profile when the primary Session Manager is unavailable. A selection is optional.                                                                                                                                            |
| <b>Origination Application Sequence</b> | <p>An Application Sequence that will be invoked when calls are routed from this user. A selection is optional.</p> <p><b>* Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p>    |
| <b>Termination Application Sequence</b> | <p>An Application Sequence that will be invoked when calls are routed to this user. A selection is optional.</p> <p><b>* Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p>      |
| <b>Conference Factory Set</b>           | <p>The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.</p> <p>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.</p>                                                                                   |

*Table continues...*

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Survivability Server</b> | <p>For local survivability, a Survivability Server can be specified to provide survivability communication services for devices associated with a Communication Profile in the event that local connectivity to Session Manager instances in the Aura is lost. If a Branch Session Manager is selected, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager survivable remote server resident with the Branch Session Manager. A selection is optional.</p> <p> <b>Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, Communication Manager associated with the application must be the main Communication Manager server for the Communication Manager survivable remote server that is resident with the Branch Session Manager.</p> |
| <b>Home Location</b>        | A Home Location to support mobility for the currently displayed user. Session Manager uses the home location when the IP address of the calling phone does not match any IP Address Pattern of any of the location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### Communication Profile tab: Avaya Breeze® platform Profile

| Name                   | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Service Profile</b> | The profile that you assign to the user. The user can gain access to the service contained in the profile. |

### Communication Profile tab — CM Endpoint Profile

 **Note:**

The system displays these fields only if a Communication Manager Endpoint profile exists for the user.

| Name/Button                   | Description                                                                                                                                                                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                 | The Communication Manager system on which you add the endpoint. You must select the system.                                                                                                                                                             |
| <b>Use Existing Endpoints</b> | The existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.                                                                                                          |
| <b>Extension</b>              | <p>The extension of the endpoint that you associate this profile with. You must select the extension.</p> <p>The field lists the endpoints, existing or available, based on the option you selected in the <b>Use Existing Endpoints</b> check box.</p> |
| <b>Template</b>               | The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add.                                                                                                                  |

*Table continues...*

| Name/Button                                              | Description                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Set Type</b>                                          | The set type of the endpoint you associate with. When you select a template, the system populates the corresponding set types.                                                                                                                                                                                                                     |
| <b>Security Code</b>                                     | The security code for authorized access to the endpoint.                                                                                                                                                                                                                                                                                           |
| <b>Port</b>                                              | The relevant port for the set type you select. You must select the port.<br>The field lists the possible ports based on the selected set type.                                                                                                                                                                                                     |
| <b>Voice Mail Number</b>                                 | The voice mail number of the endpoint you associate with.<br><br> <b>Note:</b><br>You must clear Local Device Services Data on all Avaya Aura® Web Gateway nodes if you change the value of <b>Voice Mail Number</b> .                                            |
| <b>Preferred Handle</b>                                  | Numeric only handles, SIP handles, or nonSIP handles, that are administered for a user.<br><br>The <b>Preferred Handle</b> field is optional. Select numeric handle for alphanumeric support. By default, the field is blank.<br><br>If SIP entity is of Communication Manager type, Session Manager uses preferred handle in CM Endpoint profile. |
| <b>SIP URI</b>                                           | A unique alphanumeric communication address of the user to make and receive voice or video calls. The <b>SIP URI</b> address can be: <username-projectname>@<xyz.com>.                                                                                                                                                                             |
| <b>Calculate Route Pattern</b>                           | The option to automatically select the route pattern based on the primary or secondary Session Manager configured in the <b>Session Manager Communication Profile</b> .                                                                                                                                                                            |
| <b>Sip Trunk</b>                                         | The system makes this field available only for the SIP set type.<br>If you select <b>Calculate Route Pattern</b> check box, the system: <ul style="list-style-type: none"> <li>• Populates the <b>Sip Trunk</b> field</li> <li>• Makes <b>Sip Trunk</b> field read-only.</li> </ul>                                                                |
| <b>Attendant</b>                                         | The option to enable the attendant feature on the endpoint. If you select this check box, you can administer the endpoint as an attendant.<br><br>When you select the 9641SIP template type from <b>Template</b> , the system enables the <b>Attendant</b> check box.                                                                              |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | The option to specify whether to delete the endpoint from the Communication Manager device when you remove the association between the endpoint and the user or delete the user.                                                                                                                                                                   |

*Table continues...*

| Name/Button                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Override Endpoint Name</b>                         | <p>Use this check box for the following two purposes:</p> <ul style="list-style-type: none"> <li>To override the endpoint name on Communication Manager with the value you configured on the Manage Users page during synchronization.</li> </ul> <p>If you clear the check box, the system does not override the endpoint name on Communication Manager with the name you configured in System Manager during synchronization.</p> <ul style="list-style-type: none"> <li>To override the Localized Display Name on the Manager Users page on the <b>Localized Display Name</b> field of Communication Manager.</li> </ul> <p>If you clear the check box, the system does not override the Localized display name in the <b>Localized Display Name</b> field.</p> |
| <b>Allow H.323 and SIP Endpoint Dual Registration</b> | <p>The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                   |

### Communication Profile tab - CS1000 Endpoint Profile

| Name                                  | Description                                                                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                         | The CS1000 system to which you want to add a phone.                                                                                                          |
| <b>Target</b>                         | The system customer number for the Communication Server.                                                                                                     |
| <b>Template</b>                       | The phone or endpoint template that you can choose for the user. Select a template from the drop down list. The element manager maintains all the templates. |
| <b>Update</b>                         | Updates the station profile information for the user. When you click this button, the system takes you to the element manager cut through for the updates.   |
| <b>Service Details</b>                | Displays service details of endpoints, such as set type, after phone creation.                                                                               |
| <b>Primary DN</b>                     | The primary directory number of the phone. You can enter only numeric values for this field.                                                                 |
| <b>Include in Corporate Directory</b> | Use to add this profile to the CS1K Corporate Directory feature.                                                                                             |

### Communication Profile tab — Messaging Profile

 **Note:**

You may see these fields only if a messaging profile can be configured for the user.

| Name          | Description                                                   |
|---------------|---------------------------------------------------------------|
| <b>System</b> | The Messaging System on which you need to add the subscriber. |

*Table continues...*

| Name                                                         | Description                                                                                                                                                                                       |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Template</b>                                              | The template (system defined and user defined) you want to associate with the subscriber.                                                                                                         |
| <b>Use Existing Subscriber on System</b>                     | Use this check box to specify whether to use an existing subscriber mailbox number to associate with this profile.                                                                                |
| <b>Mailbox Number</b>                                        | The mailbox number of the subscriber.<br><br>The field lists the existing subscriber if you select the <b>Use Existing Subscriber on System</b> check box.                                        |
| <b>Password</b>                                              | The password for logging into the mailbox.                                                                                                                                                        |
| <b>Delete Subscriber on Unassign of Subscriber from User</b> | Use to specify whether you want to delete the subscriber mailbox from the Messaging Device or Communication System Management when you remove this messaging profile or when you delete the user. |

### Communication Profile tab: Avaya Messaging Profile

| Name                                     | Description                                                                                                                                                                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Officelinx System</b>                 | The Avaya Messaging system to which you add a mailbox.                                                                                                                                                                                                                |
| <b>Refresh</b>                           | The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use.<br><br>You do not require to refresh for every user.                                                             |
| <b>Mailbox Number</b>                    | The mailbox number of the subscriber.                                                                                                                                                                                                                                 |
| <b>Numeric Password</b>                  | The numeric password that is used to log in to the Avaya Messaging system.                                                                                                                                                                                            |
| <b>Confirm Numeric Password</b>          | The numeric password that you retype to confirm.                                                                                                                                                                                                                      |
| <b>Application User Password</b>         | The password that is used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.                                                                                                                       |
| <b>Confirm Application User Password</b> | The password that you retype to confirm.                                                                                                                                                                                                                              |
| <b>Company</b>                           | The name of the company to which the user belongs.                                                                                                                                                                                                                    |
| <b>Department</b>                        | The department to which the user belongs.                                                                                                                                                                                                                             |
| <b>Feature Group</b>                     | The feature group name that determines the rules for the mailboxes associated with it.                                                                                                                                                                                |
| <b>Capability</b>                        | The type of functionality that the user contains. The values are: <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Fax</b></li> <li>• <b>Messaging</b></li> <li>• <b>Collaboration</b></li> <li>• <b>Messaging and Collaboration</b></li> </ul> |
| <b>Domain Account Name</b>               | The mailbox NT account name of the Avaya Messaging profile.                                                                                                                                                                                                           |

*Table continues...*



| Name                             | Description                                                                                                         |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Synchronization User Name</b> | The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail. |

**\* Note:**

Only one-way update is supported for Officelinx elements. If you make any change directly on Officelinx, it does not reflect on System Manager. If you edit the user from System Manager, it overrides the changes you made directly on Officelinx.

### Communication Profile tab — IP Office Endpoint Profile

Use this profile to assign a new or an existing user to a System Manager device in User Management.

While adding a user, if you choose to assign a CM endpoint profile and an IP Office endpoint profile to the user, then the system uses the IP Office endpoint profile as the survivability option for the CM endpoint profile. That is, the endpoint extension used in the CM endpoint profile is also used for creating an IP Office endpoint profile so that when Communication Manager is unavailable, the IP Office device can serve the extension.

**\* Note:**

If a Communication Manager endpoint profile is present while adding or editing a user, the user administration functions in the centralized mode. If a Communication Manager endpoint profile is present, the user administration functions in the distributed mode.

Commit the Communication Manager endpoint profile and the Session Manager endpoint profile before you add an IP Office endpoint profile for a centralized user.

| Name/Button                   | Description                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                 | Displays a list of IP Office device names from which you can select the IP Office device you want to associate with the user.                                                                                                                                                                        |
| <b>Template</b>               | Displays a list of user templates from which you can select your preferred template to set the user configurations.                                                                                                                                                                                  |
| <b>Use Existing Extension</b> | Select the check box to use an existing endpoint extension to associate with this profile. If you do not select this check box, the system uses the available extensions.                                                                                                                            |
| <b>Extension</b>              | The extension of the endpoint you want to associate.<br><br>The field lists the endpoints, existing or available, based on option you selected in the <b>Use Existing Endpoints</b> check box.                                                                                                       |
| <b>Endpoint Editor</b> button | Launches the IP Office application, where you can edit or view details of the IP Office endpoint.<br><br>After you save the changes in IP Office, the system does not update the modified data on the device or database until you commit the changes on the User Profile   Edit   <User Name> page. |
| <b>Module-Port</b>            | The module port combination list for IP Office analog extensions. You must select <b>Module-Port</b> for centralized users with Set Type as <b>Analog</b> .                                                                                                                                          |

*Table continues...*

| Name/Button                                      | Description                                                                                                                                                                                                                                        |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Set Type</b>                                  | Displays the set type for the IP Office endpoint profile. By default, the <b>Set Type</b> field is disabled. If you select a template, the set type is auto populated.                                                                             |
| <b>Delete Extension On User Delete</b> check box | Provides the option to delete the extension associated with the user while deleting the user. By default, this check box is clear. This option is available for communication profiles associated with <b>Analog</b> and <b>Digital</b> set types. |

### Communication Profile tab: Equinox Conferencing

| Name                         | Description                                  |
|------------------------------|----------------------------------------------|
| <b>Equinox User Password</b> | The Equinox user password.                   |
| <b>Virtual Room Number</b>   | The virtual room number of the Equinox user. |

### Communication Profile tab — Presence Profile

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                              | The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: <ul style="list-style-type: none"> <li>• Aggregate presence</li> <li>• Archive instant messages if the Instant Messages option is enabled</li> </ul>      |
| <b>SIP Entity</b>                          | The option to route the SIP-based messages through Presence Services. This system selects the SIP entity only if you select a Presence Services instance in the <b>System</b> field. <b>SIP Entity</b> is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.                                                                |
| <b>IM Gateway SIP Entity</b>               | The Presence Services instance for the user.                                                                                                                                                                                                                                                                                                                                            |
| <b>Publish Presence with AES Collector</b> | The option that determines if Presence Services must publish presence with AES Collector. The options are: <ul style="list-style-type: none"> <li>• <b>System Default</b></li> <li>• <b>Off</b></li> <li>• <b>On</b></li> </ul> The default is <b>System Default</b> . You can change the default value. You do not require to configure AES Collector in the Presence Services server. |

## Communication Profile tab: Conferencing Profile

| Name                                                         | Description                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Auto-generated Code Length</b>                     | The number of characters in PIN. The default is 6.<br><br>The system displays this field if you select the <b>Auto Generate Participant and Moderator Security Code</b> check box.                                                                             |
| <b>Auto Generate Participant and Moderator Security Code</b> | Select the check box if the system must generate the participant security code and moderator security code for this user.<br><br>Clear the check box to assign a specific participant security code or moderator security code for this user.                  |
| <b>Participant Security Code</b>                             | The participant security code that you assign for this user.<br><br>The system displays this field only when the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.                                                              |
| <b>Moderator Security Code</b>                               | The moderator security code that you assign for this user.<br><br>The system displays this field if the <b>Auto Generate Participant and Moderator Security Code</b> check box is clear.                                                                       |
| <b>Location</b>                                              | The location of the user. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.<br><br>For SIP users, the system uses the location value from the <b>Home Location</b> field in the Session Manager profile. |
| <b>Template</b>                                              | The Conferencing template that you assign to this user.                                                                                                                                                                                                        |

| Button               | Description                                                                     |
|----------------------|---------------------------------------------------------------------------------|
| <b>Get Templates</b> | Displays the list of Conferencing templates, which you can assign to this user. |

## Communication Profile tab: Work Assignment Profile

| Name                   | Description          |
|------------------------|----------------------|
| <b>Account</b>         | The account name.    |
| <b>Account Address</b> | The account address. |
| <b>Source</b>          | The source name.     |
| <b>Source Address</b>  | The source address.  |

When you click **Resource Details**, **Account Details**, or **Source Details**, the system displays the Assignment Management page in Work Assignment.

| Button                  | Description                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Resource Details</b> | Displays the Assignment Management page where you can configure assignment targets for the user.<br><br>You can assign resource details to an agent only when the user has the Work Assignment profile assigned to the user. |

*Table continues...*

| Button                 | Description                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Account Details</b> | Displays the text box where you can add or modify the account name and account address.<br><br>You can add attributes to the account only when the account is added to the agent.     |
| <b>Source Details</b>  | Displays the text box where you can add or modify the source name and source address.<br><br>You can add properties and attributes to the source only when the source already exists. |

### Membership tab — Roles section

| Name               | Description                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>check box</b>   | Use this check box to select a role. Use the check box displayed in the first column of the header row to select all the roles assigned to the user account. |
| <b>Name</b>        | The name of the role.                                                                                                                                        |
| <b>Description</b> | A brief description about the role.                                                                                                                          |

| Button                | Description                                                                        |
|-----------------------|------------------------------------------------------------------------------------|
| <b>Assign Roles</b>   | Opens the Assign Role page that you can use to assign roles to the user account.   |
| <b>UnAssign Roles</b> | Removes the selected role from the list of roles associated with the user account. |

### Membership tab — Group Membership section

| Name               | Description                             |
|--------------------|-----------------------------------------|
| <b>check box</b>   | Use this check box to select the group. |
| <b>Name</b>        | Name of the group.                      |
| <b>Type</b>        | Group type based on the resources.      |
| <b>Hierarchy</b>   | Position of the group in the hierarchy. |
| <b>Description</b> | A brief description about the group.    |

| Button                   | Description                                                               |
|--------------------------|---------------------------------------------------------------------------|
| <b>Add To group</b>      | Opens the Assign Groups page that you can use to add the user to a group. |
| <b>Remove From Group</b> | Removes the user from the selected group.                                 |

## Contacts tab — Default Contact List

| Name               | Description                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | Name of the contact list. The default name of the contact list is Default. You can change the name to any other appropriate name. |
| <b>Description</b> | A brief description of the contact list.                                                                                          |

## Contacts tab — Associated Contacts

| Name                    | Description                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>        | Last name of the contact.                                                                                                                                               |
| <b>First Name</b>       | First name of the contact.                                                                                                                                              |
| <b>Scope</b>            | Categorization of the contact based on whether the contact is a public or private contact.                                                                              |
| <b>Speed Dial</b>       | The value specifies whether the speed dial is set for the contact or not.                                                                                               |
| <b>Speed Dial Entry</b> | The reduced number that represents the speed dial number.                                                                                                               |
| <b>Presence Buddy</b>   | The value specifies whether you can monitor the presence information of the contact or not. A false value indicates that you can not track the presence of the contact. |

| Button             | Description                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>        | Opens the Edit Contact List Member page. Use this page to modify the information of the selected contact.                   |
| <b>Add</b>         | Opens the Attach Contacts page. Use this page to select one or more contacts from the list of contacts.                     |
| <b>Remove</b>      | Removes one or more contacts from the list of the associated contacts.                                                      |
| <b>Filter menu</b> | You can find the <b>Filter menu</b> icon next to the name of each column.<br>Filters the data based on the search criteria. |

## Contacts tab — Private Contacts

Use this section to add new private contacts, modify and deletes existing contacts.

| Name                   | Description                            |
|------------------------|----------------------------------------|
| <b>Last Name</b>       | Last name of the private contact.      |
| <b>First Name</b>      | First name of the private contact.     |
| <b>Display Name</b>    | Display name of the private contact.   |
| <b>Contact Address</b> | Address of the private contact.        |
| <b>Description</b>     | A brief description about the contact. |

| Button      | Description                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Opens the Edit Private Contact page. Use this page to modify the information of the selected contact. |

*Table continues...*

| Button             | Description                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>New</b>         | Opens the New Private Contact page. Use this page to add a new private contact.                                             |
| <b>Delete</b>      | Deletes the selected contacts.                                                                                              |
| <b>Filter menu</b> | You can find the <b>Filter menu</b> icon next to the name of each column.<br>Filters the data based on the search criteria. |

### Common buttons

| Button                       | Description                                                                                             |
|------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Commit &amp; Continue</b> | Duplicates the user account and retains you on the same page for further modifications.                 |
| <b>Commit</b>                | Duplicates the user account and takes you to the User Management page.                                  |
| <b>Cancel</b>                | Cancels the operation of modifying the user information and takes you back to the User Management page. |

## User Delete Confirmation field descriptions

| Name                | Description                                                                    |
|---------------------|--------------------------------------------------------------------------------|
| <b>Last Name</b>    | The last name of the user.                                                     |
| <b>First Name</b>   | The first name of the user.                                                    |
| <b>Display Name</b> | The localized display name of a user. It is typically the localized full name. |
| <b>Login Name</b>   | The login name of the you want to delete.                                      |
| <b>Last login</b>   | The date and time of last successful login on to System Manager.               |

| Button        | Description                                                                       |
|---------------|-----------------------------------------------------------------------------------|
| <b>Delete</b> | Deletes the user.                                                                 |
| <b>Cancel</b> | Closes the User Delete Confirmation page and returns to the User Management page. |

## Assign Roles to Multiple Users field descriptions

### Selected Users

| Name                | Description                             |
|---------------------|-----------------------------------------|
| <b>Last Name</b>    | The last name of the user.              |
| <b>First Name</b>   | The first name of the user.             |
| <b>Display Name</b> | The localized display name of the user. |

*Table continues...*

| Name       | Description                                                  |
|------------|--------------------------------------------------------------|
| User Name  | The unique name that gives access to the system .            |
| Last login | The time and date when the user has logged in to the system. |

### Select Roles

| Name             | Description                         |
|------------------|-------------------------------------|
| Select Check box | The option to select a role.        |
| Name             | The name of the role.               |
| Description      | A brief description about the role. |

| Button | Description                                                                    |
|--------|--------------------------------------------------------------------------------|
| Commit | Assigns roles to the selected users.                                           |
| Cancel | Cancels the role assignment operation and returns to the User Management page. |

## Assign Roles field descriptions

### Selected Roles

The section displays roles that you have assigned to the user account.

| Name        | Description                                           |
|-------------|-------------------------------------------------------|
| Name        | The roles that you have assigned to the user account. |
| Description | A brief description about the roles.                  |

### Available Roles

The table in this section displays roles that you can assign to the user account.

| Name             | Description                                        |
|------------------|----------------------------------------------------|
| Select check box | The option to select all the roles in the table.   |
| Name             | The roles that you can assign to the user account. |
| Description      | A brief description of the roles.                  |

| Button | Description                                                             |
|--------|-------------------------------------------------------------------------|
| Select | Assigns the selected roles to the user.                                 |
| Cancel | Cancels the role assignment operation and returns to the previous page. |

---

## Assign Groups field descriptions

### Selected Groups

The section displays groups that are assigned to the user.

| Name        | Description                                 |
|-------------|---------------------------------------------|
| Name        | The name of the group.                      |
| Type        | The group type based on the resources.      |
| Hierarchy   | The position of the group in the hierarchy. |
| Description | A brief description of the group.           |

### Available Groups

The table in this section displays groups that you can assign to the user account.

| Name             | Description                                 |
|------------------|---------------------------------------------|
| Select check box | The option to select a group.               |
| Name             | The name of the group.                      |
| Type             | The group type based on the resources.      |
| Hierarchy        | The position of the group in the hierarchy. |
| Description      | A brief description of the group.           |

| Button       | Description                              |
|--------------|------------------------------------------|
| Select       | Assigns the selected groups to the user. |
| Cancel       | Cancels the group assignment operation.  |
| Select: ALL  | Selects all groups in the table.         |
| Select: None | Clears the selection.                    |

---

## Assign Groups to Multiple Users field descriptions

Use this page to add users to a group.

### Selected Users

| Name         | Description                                                   |
|--------------|---------------------------------------------------------------|
| Last Name    | The last name of the user.                                    |
| First Name   | The first name of the user.                                   |
| Display Name | The localized display name of the user.                       |
| User Name    | The unique name that gives access to the system.              |
| Last login   | The time and date when the user last logged on to the system. |



## Select Groups

| Name             | Description                                  |
|------------------|----------------------------------------------|
| Select check box | The option to select a group.                |
| Name             | The name of the group.                       |
| Type             | The group type based on the resources.       |
| Hierarchy        | The position of the group within the groups. |
| Description      | A brief description of the group.            |

| Button       | Description                                                                     |
|--------------|---------------------------------------------------------------------------------|
| Select: All  | Selects all groups displayed in the table.                                      |
| Select: None | Clears the selected check boxes.                                                |
| Commit       | Assigns groups to the selected users.                                           |
| Cancel       | Cancels the group assignment operation and returns to the User Management page. |

## Deleted Users field descriptions

You can view the users that you have deleted using the Delete feature. Use this page to view, permanently delete a user, and restore users that you have deleted.

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select check box       | The option to select a group.                                                                                                                                                                                                                                                                                                                               |
| Last Name              | The last name of the deleted user.                                                                                                                                                                                                                                                                                                                          |
| First Name             | The first name of the deleted user.                                                                                                                                                                                                                                                                                                                         |
| Display Name           | The localized display name of the deleted user.                                                                                                                                                                                                                                                                                                             |
| Login Name             | The unique name that identifies the user in the system.                                                                                                                                                                                                                                                                                                     |
| Organization Hierarchy | <p>The hierarchy of the tenant organization in the format Tenant/Site/Department/Team.</p> <p>For example, Citi/Pune/HomeLoans/LoanSupport.</p> <p> <b>Note:</b></p> <p>The system displays the field only when the administrator enables the Multi Tenancy feature.</p> |
| Last login             | The time and date when the user last logged on to the system.                                                                                                                                                                                                                                                                                               |

| Button             | Description                                             |
|--------------------|---------------------------------------------------------|
| Delete             | Deletes the user permanently from the database.         |
| Restore            | Restores the deleted user.                              |
| Show Regular users | Returns to the User page and displays the active users. |

## User Restore Confirmation field descriptions

Use this page to restore a deleted user.

| Name                          | Description                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>              | The last name of the user.                                                                                                                                                                                                                                                                                                                                |
| <b>First Name</b>             | The first name of the user.                                                                                                                                                                                                                                                                                                                               |
| <b>Display Name</b>           | The localized display name of the user.                                                                                                                                                                                                                                                                                                                   |
| <b>Login Name</b>             | The unique name of the user account.                                                                                                                                                                                                                                                                                                                      |
| <b>Organization Hierarchy</b> | <p>The hierarchy of the tenant organization in the format Tenant/Site/Department/Team.</p> <p>For example, Citi/Pune/HomeLoans/LoanSupport.</p> <p> <b>Note:</b></p> <p>The system displays the field only when the administrator enables the Multi Tenancy feature.</p> |
| <b>Last login</b>             | The date and time when the user last logged on to the system.                                                                                                                                                                                                                                                                                             |

| Button         | Description                                                                               |
|----------------|-------------------------------------------------------------------------------------------|
| <b>Restore</b> | Removes the user from the list of deleted users and restores the user as an active user.  |
| <b>Cancel</b>  | Closes the User Restore Confirmation page and returns you back to the Deleted Users page. |

## Assign Users To Roles field descriptions

Use this page to assign one or more users to the selected roles. This page has the following two sections:

- Selected Roles
- Select Users

### Selected Roles section

The roles to which you can assign users.

| Name                 | Description                                                         |
|----------------------|---------------------------------------------------------------------|
| <b>Name</b>          | Displays the name of the role.                                      |
| <b>Resource Type</b> | Displays the resource type that the corresponding role is assigned. |
| <b>Description</b>   | Displays a brief description about role.                            |

### Select Users section

The table displays the users to which you can assign the roles.

| Name                    | Description                                                            |
|-------------------------|------------------------------------------------------------------------|
| <b>Select check box</b> | Provides the option to select the user.                                |
| <b>Last Name</b>        | Displays the last name of the user.                                    |
| <b>First Name</b>       | Displays the first name of the user.                                   |
| <b>Display Name</b>     | The display name of the user.                                          |
| <b>User Name</b>        | Displays the unique name that identifies the user.                     |
| <b>Last Login</b>       | Displays the time and date when the user last logged on to the system. |

| Button        | Description                                                              |
|---------------|--------------------------------------------------------------------------|
| <b>Commit</b> | Assigns user to the role.                                                |
| <b>Cancel</b> | Cancels the assign users operation and returns to the Manage Roles page. |

## UnAssign Roles field descriptions

### Selected Roles

The role from which users are unassigned.

| Name                 | Description                                  |
|----------------------|----------------------------------------------|
| <b>Name</b>          | The name of the role.                        |
| <b>Resource Type</b> | The resource type that the role is assigned. |
| <b>Description</b>   | A brief description of the role.             |

### Select Users

The table displays the users for which you can remove the roles.

| Name                    | Description                                                   |
|-------------------------|---------------------------------------------------------------|
| <b>Select check box</b> | The option to select the user.                                |
| <b>Last Name</b>        | The last name of the user.                                    |
| <b>First Name</b>       | The first name of the user.                                   |
| <b>Display Name</b>     | The display name of the user.                                 |
| <b>User Name</b>        | The unique name that identifies the user.                     |
| <b>Last Login</b>       | The time and date when the user last logged on to the system. |

| Button        | Description                                                              |
|---------------|--------------------------------------------------------------------------|
| <b>Commit</b> | Unassigns the role from the users.                                       |
| <b>Cancel</b> | Cancels the assign users operation and returns to the Manage Roles page. |

---

## Managing bulk import and export

### Bulk import and export

In System Manager, you can import and export user profiles and global settings in bulk. To import data in bulk, you must provide an XML file or an Excel file as input file. System Manager validates any file that you upload during the bulk import operation.

System Manager filters uploaded files based on the file extension and mime type or bytes in the file.

The system exports the data to an XML file and an Excel file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity data
- Communication profile set
- Handles
- Communication profiles

The supported communication profiles are CM Endpoint, CM Agent, Messaging, Session Manager, CS 1000 Endpoint, Conferencing, IP Office, Presence, Avaya Breeze® platform, Work Assignment, Avaya Messaging, and Avaya Meetings Server.

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

#### Important:

System Manager does not support import and export of roles in bulk.

### Bulk import and export using the Excel file

In System Manager, you can import and export user profiles in bulk by using an Excel file and an XML file. To import data in bulk, provide an XML file or an Excel file as input that System Manager supports. When you export the data from the System Manager web console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the .xlsx format. You can download the Excel file from the User Management page.

Importing and exporting in bulk by using the Excel template provides the following features:

- Supports the following types of user information:
  - Basic. The identity attributes of the user that include user provisioning rule name for the user, the tenant, and organization hierarchy details
  - Profile Set. Entries for all communication profile sets for all users

The Profile Set sheet contains an entry for each communication profile set for a user. The user must set only one communication profile set as *true* for a user in the **Is Default** column. The value *true* indicates that the communication profile set of the user is the default.

- Handle. The communication address of the user
- Session Manager profile
- Avaya Breeze® platform profile
- CM Endpoint profile with all attributes of the station communication profile
- CM Agent profile with all attributes.
- Messaging profile
- Avaya Messaging profile
- IP Office Endpoint profile
- CS 1000 Endpoint profile
- Presence profile
- Conferencing profile
- Work Assignment profile
- Avaya Meetings Server profile
- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user by using the same Excel file. However, you can only perform one operation at a time.
- For updation, supports only the partial merge operation.

Bulk import and export by using Excel does not support complete or partial replace of the user for imports in bulk.

Bulk import and export by using Excel supports a subset of user attributes that XML supports. For example, Excel does not support user contacts, address, and roles.

## The Excel file

The sample Excel file contains the sample data of some key attributes of the user. The Excel file provides a description of header fields. When you download the Excel template from the User Management page, the values remain blank. To use the Excel file, export some users for reference in an Excel file.

The login name in the **Basic** worksheet is the key attribute that you use to link the user records in other worksheets.

The login name of the user and the profile set name in the **Profile Set** worksheet are used to link to the user records in other worksheets for that user profile.

- Although you can edit the header fields in the Excel template, do not change any details of any headers in the worksheets. The import or export might fail if you change the details of the header.
- Do not change the column position in the Excel file or the structure of the Excel template.

- Do not sort the data in worksheets.

## CM Endpoint communication profile

The Excel file contains all attributes for the CM station endpoint profile that are spread in different worksheets. The parent sheet provides a link to the same user profile record in the child worksheet. The link points to the first record in the child sheet if the user profile contains multiple records in the child worksheet.

### Related links

[Downloading the Excel template file](#) on page 381

[Microsoft Excel data link error](#) on page 375

[Examples of bulk import and export of user by using the Excel file](#) on page 372

[Hierarchy in communication profile worksheets](#) on page 374

## Examples of bulk import and export of user by using the Excel file

The following are the credentials of John Miller, a user with two communication profile sets:

- Login name: johnmiller@avaya.com
- Name of the default communication profile set: Primary
- Name of the nondefault communication profile set: secondaryProfile

### Example of navigation across Excel worksheets

In the exported file, you can use the hyperlink to navigate across worksheets to access various records for a profile data of a user.

In the **CM Endpoint Profile** worksheet, the **Station Site Data** and **Buttons** columns contain hyperlinks to navigate to the respective worksheets. If the child worksheet, for example, **Buttons** contains only one record in the worksheet for that user profile, the link points to the corresponding record of the user profile. If the child worksheet contains multiple records for that user profile, the link points to the first record in the list.

| Login Name*                  | ..... | Station Site Data                                 | Abbr List | Buttons                                 |
|------------------------------|-------|---------------------------------------------------|-----------|-----------------------------------------|
| johnmiller@avaya.com#Primary | ..... | <a href="#">Go to Station Site Data worksheet</a> |           | <a href="#">Go to Buttons worksheet</a> |

In the following **Station Site Data** worksheet, the link points to the corresponding user profile record of the child worksheet because this child worksheet contains only one record for that user profile.

| Login Name*                  | Room | Jack | Cable | Floor | Building | Headset | Speaker | Mounting | Cord Length | Set Color |  |
|------------------------------|------|------|-------|-------|----------|---------|---------|----------|-------------|-----------|--|
| johnmiller@avaya.com#Primary |      |      |       |       |          | false   | false   | d        | 0           |           |  |

The following **Buttons** worksheet contains multiple records for johnmiller@avaya.com#Primary, the user profile, but the link points to the first record in the list.

| Login Name*                  | Number* | Type*     | Data1 | Data2 | Data3 | Data4 | Data5 | Data6 |
|------------------------------|---------|-----------|-------|-------|-------|-------|-------|-------|
| johnmiller@avaya.com#Primary | 1       | call-appr |       |       |       |       |       |       |
| johnmiller@avaya.com#Primary | 2       | call-appr |       |       |       |       |       |       |
| johnmiller@avaya.com#Primary | 3       | call-appr |       |       |       |       |       |       |

### Example of handling multiple communication profile sets for a user

In the exported Excel file, the system appends the login name with #profileSetName in all worksheets except the **Basic** and **Profile Set** worksheets. Appending the profile set name to the login name associates the communication profile set with the user record, for example, jmiller@avaya.com#profileSetName. When you export users in the Excel file, the association is automatic. When you provide data in a blank Excel template that you downloaded for import, you must make the association manually.

#### \* Note:

The **Profile Set** worksheet must contain all communication profile sets of a user, but only one communication profile set can be the default. The **Is Default** column is set to `true` only for the default profile.

In the **Profile Set** worksheet, the two communication profile sets for the user John Miller must contain the following information:

| Login Name*          | Name*            | Is Default* |
|----------------------|------------------|-------------|
| johnmiller@avaya.com | secondaryProfile | false       |
| johnmiller@avaya.com | Primary          | true        |

If a SIP e164 handle is associated with secondaryProfile of John Miller, the **Handle** worksheet must contain the following information:

| Login Name*                           | Handle* | Type* | Sub Type | Domain            |
|---------------------------------------|---------|-------|----------|-------------------|
| johnmiller@avaya.com#secondaryProfile | +1123   | sip   | e164     | smgrdev.avaya.com |

If a Session Manager communication profile is associated with secondaryProfile of John Miller, the **Session Manager Profile** worksheet must contain the following information:

| Login Name*                           | Type*           | Session Manager | Session Manager | Termination Application Sequence | Origination Application Sequence | Conference Factory Set | Survivability Server | Home Location* | Max. Simultaneous Devices | Block New Registration When Max Active | Enable Disable Call Log |
|---------------------------------------|-----------------|-----------------|-----------------|----------------------------------|----------------------------------|------------------------|----------------------|----------------|---------------------------|----------------------------------------|-------------------------|
| johnmiller@avaya.com#secondaryProfile | Session Manager | sm6             |                 |                                  |                                  |                        |                      | Pune           | 6                         | false                                  | true                    |

If a Avaya Breeze® platform communication profile is associated with Primary for John Miller, the **CE Profile** worksheet must contain the following:

| Login Name*                  | Type* | Service Profile* |
|------------------------------|-------|------------------|
| johnmiller@avaya.com#Primary | AUS   | TempProfile      |

## Hierarchy in communication profile worksheets

The table provides the parent-child relation of communication profile worksheets in the Excel template for bulk import and export of user.

| Element                          | Master worksheet        | Child worksheets                                                                                                                                                                                                                                                                                                                         |
|----------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Session Manager                  | Session Manager Profile | None                                                                                                                                                                                                                                                                                                                                     |
| Communication Manager — Endpoint | CM Endpoint Profile     | <ul style="list-style-type: none"> <li>• Station Site Data</li> <li>• Buttons</li> <li>• Feature Buttons</li> <li>• Expansion Module Buttons</li> <li>• Soft Keys</li> <li>• Display Buttons</li> <li>• Station Abbr Dialing Data</li> <li>• Station Data Module</li> <li>• Station Hot Line Data</li> <li>• Native Name Data</li> </ul> |
| Communication Manager — Agent    | CM Agent Profile        | <ul style="list-style-type: none"> <li>• CM Agent LoginId Skills Data</li> <li>• CM Agent Native Name Data</li> </ul>                                                                                                                                                                                                                    |

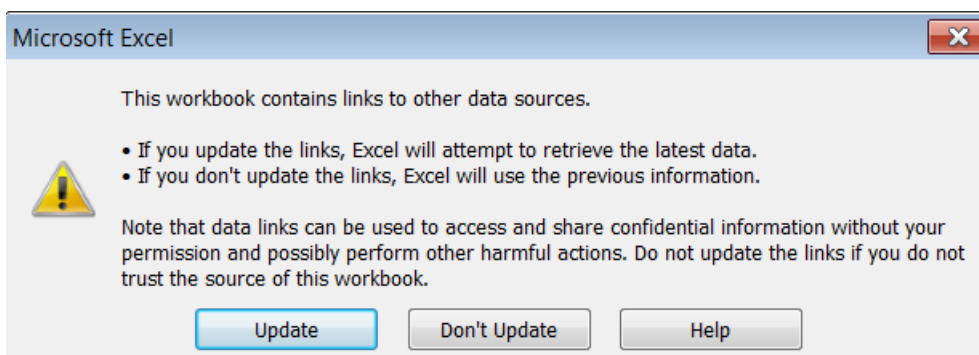
*Table continues...*



| Element                | Master worksheet           | Child worksheets                                                                                                                           |
|------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Messaging              | Messaging Profile          | <ul style="list-style-type: none"> <li>• Messaging MMSpecific</li> <li>• Messaging CMMSpecific</li> <li>• Messaging AAMSpecific</li> </ul> |
| Conferencing           | Conferencing Profile       | None                                                                                                                                       |
| IP Office              | IP Office Endpoint Profile | None                                                                                                                                       |
| CS 1000                | CS 1000 Endpoint Profile   | None                                                                                                                                       |
| Avaya Breeze® platform | CE Profile                 | None                                                                                                                                       |
| Presence               | Presence Profile           | None                                                                                                                                       |
| Work Assignment        | Work Assignment Profile    | <ul style="list-style-type: none"> <li>• Work Assignmnt Resource Details</li> <li>• Work Assignmnt Agent Attributes</li> </ul>             |
| Avaya Messaging        | Avaya Messaging Profile    | None                                                                                                                                       |
| Equinox                | Equinox Profile            | None                                                                                                                                       |

## Microsoft Excel data link error

Microsoft Excel 2010 displays a data link error.



### Related links

[Proposed solution](#) on page 375

## Proposed solution

### About this task

You can ignore Data link error that Microsoft Excel 2010 displays. However, perform the following procedure to avoid this error the next time you open an Excel file.

### Procedure

1. On the Excel worksheet, close the warning message.
2. On the **Data** menu, click **Edit Links**.
3. On the Edit Links dialog box, click **Startup Prompt**.
4. Click **Don't display the alert and don't update automatic links** and click **OK**.

5. Click **Close**.
6. Save the Excel file.
7. Close the Excel file and open the file again.

The system does not display the data link error message now.

#### Related links

[Proposed solution](#) on page 375

## Data entry warning in Microsoft Excel

The data type of the cell in Excel is text. If you provide a number in the cell, Excel displays the `Number Stored as Text` message. Ignore the warning and do not change the data type of the cell.

#### Related links

[Proposed solution](#) on page 376

## Proposed solution

### About this task

You can ignore data entry warning that Microsoft Excel 2007 or later displays. However, perform this procedure to turn off the warning message.

### Procedure

1. Based on the version, do one of the following:
  - In Microsoft Office Excel 2007, click **Excel Options**.
  - In Microsoft Office Excel 2010, click **File > Options > Excel Options**.For other Microsoft Office Excel versions, use the appropriate options.
2. In Microsoft Office Excel 2010, in the left navigation pane, click **Formulas** and clear the **Numbers formatted as text or preceded by an apostrophe** check box.
3. Click **OK**.

## Key features of bulk import and bulk export

- Supports import of user profiles from an XML file and Excel file, and import of global settings from an XML file. Also, supports the export of data to an XML file and Excel file.
- Supports the following error configurations:
  - Abort on first error. Stops the import of user records when the import user operation encounters the first error in the import file containing the user records.
  - Continue processing other records. Imports the next user record even if the import user operation encounters an error while importing a user record.
- Supports the following import types:
  - A *Partial Import* type helps import of users with specific user attributes.

- A *Complete Import* helps import of users with all user attributes.
- Provides various configuration options if a record that you must import matches an existing record in the database. You can configure to skip, replace, merge, or delete a matching record that already exists and reimport data.
- Supports scheduling of bulk import jobs from System Manager Web Console.
- Displays import job details, such as job scheduled time, job end time, job status, job completion status in percentage, number of user records in the input file, number of user records in the input file with warnings, and number of user records in the input file that failed to import. Also, provides the link to the Scheduler user interface.
- Supports cancellation and deletion of an import job.
- Maintains logs of records that fail to import and that require manual intervention.
- Supports download of failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and reimport the records into the database.

## About bulk import of users

You can use the bulk import functionality to import users in bulk with their attributes from an XML file. The XML file must conform to XML schema definition. For more information, see [XML Schema Definition for bulk import of users](#) on page 408. See [Sample XML for bulk import of users with all attributes](#) on page 415 for the sample XML file for bulk import of user.

You can perform the following tasks with the bulk import functionality:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform the following import types:
  - A *Partial* import type helps import of users with specific user attributes.
  - A *Complete* import type helps import of users with all user attributes.
- Skip import of the users that already exist in the database. Use this option to import new users from the XML file.
- Replace the users in the database with the new users from the file you imported. The system performs the following actions:
  - Replaces all items of user collection attributes such as CommprofileSet and Contactlist.
  - Removes the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofilesset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commprofiles StationC and EndpointB in the default commprofilesset.

 **Note:**

For CS1000 Endpoint Profile, you cannot import both communication profile and user at the same time. You must add the user and then merge the profile.

- Update and merge the user attributes data from the imported file to the existing data. The system performs the following actions:
  - Merges items of user collection attributes such as CommprofileSet and Contactlist.
  - Retains and updates the existing items.
  - Adds the new items from the XML.
  - Updates the single-value user attributes.

For example, the user John Miller has StationA and EndpointB as existing commprofiles in default commprofilesset and you import an XML file containing users with StationC and EndpointB with *Replace* option. After you import, John Miller has commProfiles StationA, StationC, EndpointB in the default commprofilesset.

- Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

The following two XML schema definitions are available based on the complete and partial import types:

- XML schema definition for bulk import of users: See [XML Schema Definition for bulk import of users](#) on page 408. Use this XML schema definition to add and update (Merge/Replace) users. This schema addresses complete user attributes. For a sample XML that conforms to the XML schema definition, see [Sample XML for bulk import of users with minimal attributes](#) on page 415 and [Sample XML for bulk import of users with all attributes](#) on page 415.

- XML schema definition for partial import of users: See [XML Schema Definition for partial import of user attributes](#) on page 423. Use the XML schema definition to add and update (Merge/Replace) users. You must use this schema to import users with specific user attributes. For a sample XML that conforms to this XML schema definition, see [Sample XML for partial import of user attributes](#) on page 425.

To delete bulk users, a separate XML schema definition is defined. See [XML Schema Definition for bulk deletion of users](#) on page 427. For a sample XML that conforms to delete bulk users XML schema definition, see [Sample XML for bulk deletion of users](#) on page 428.

## Configuration options for bulk import using Excel

You can bulk import only the supported user attribute data for users. The Excel file must be the downloaded Excel template file or exported Excel file.

The following configuration options are available for import of users by using the Excel file:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Import users with specific or all user attributes that Excel supports.
- If a matching record already exists, you can:
  - Merge the user attribute data from the imported file to the existing data. For example, you can add a new handle to the existing user.
  - Delete the user records from the database that match the records in the input Excel file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.

## Bulk importing of users

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.

2. Click **Import > User Management > Users**.

Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.

3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:

- XML
- Excel

 **Note:**

Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release`. Use the Excel template that you downloaded or exported from the current System Manager release.

4. On the Import users page, in the **Select File** field, type the complete path of the file or click **Browse** to locate and select a file.

5. Select one of the following error configuration options:

- **Abort on first error**
- **Continue processing other records**

6. For the XML file type, click **Complete** in the import type.

If you select the Excel file type, the system does not display the import type option.

7. Select one of the following import options:

- To skip users in the import file that match the existing user records in the database, click **Skip**.
- To replace the users in the database with new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.  
If you select Excel file type, the system does not display the replace option
- To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
- To delete the user records in the database that match the records in the imported file, click **Delete**.

 **Note:**

For import by using Excel, the system deletes the user records permanently.

8. To run the job, in the Job Schedule section, select one of the following:

- To import the users immediately, click **Run immediately**.
- To import the users at a specified time, click **Schedule later**, and set date and time.

## 9. Click **Import**.

If you use the default configurations option **Importing Users > Add Users** in the database, the system imports the next user record even if the import user operation encounters an error while importing a user record. The system logs an error. Skip import of users that already exist in the database. The system schedules the import job to run immediately.

### **Note:**

The operations, Communication Manager synchronization and bulk import of users, must not overlap in time. When bulk import of users is in progress and if Communication Manager synchronization starts, the records that are in process fail. When synchronization is complete, the remaining bulk import records process successfully. You must reimport the records that fail to import during synchronization.

### Related links

[Attribute details defined in Import user XSD](#) on page 524

[Attribute details defined in Delete User XSD](#) on page 535

[Attribute details defined in the CM Endpoint profile XSD](#) on page 536

[Attribute details defined in the Messaging communication profile XSD](#) on page 565

[Attribute details defined in the Session Manager communication profile XSD](#) on page 574

[Downloading the Excel template file](#) on page 381

[Microsoft Excel data link error](#) on page 375

## Downloading the Excel template file

### About this task

To import or export by using an Excel file, you must use the Excel template file that System Manager supports. System Manager validates and displays a message if you use an unsupported Excel file.

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, click **More Actions > Download Excel Template**.
4. In the Opening <Excel template file name>.xlsx dialog box, click **Save File**, and click **OK**.

### **Important:**

Though the header fields in the Excel template are editable, do not change any header information in the worksheets. The import or export might fail if you modify the headers.

For the sample Excel template, see the Excel template for bulk import and export that you download from the User Management page.

## Bulk export of users

In System Manager, you can export users in bulk from the System Manager database. While exporting in bulk, the system exports the data to an XML file.

You can export the following user attributes in bulk:

- Identity data
- Communication profile set
- Handles
- Communication profiles

The supported communication profiles are CM Endpoint, CM Agent, Messaging, Session Manager, CS 1000 Endpoint, Conferencing, IP Office, Presence, Avaya Breeze<sup>®</sup> platform, Work Assignment, Avaya Messaging, and Avaya Meetings Server.

### **Note:**

For security reasons, the system does not export the password fields in the XML file.

You can export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

The Export User process creates an archive file containing one or more XML files. While exporting users records, if the number of exported records exceed the limit of records that an XML file can hold, the system creates multiple XML files. The system packages the XML files in a zip file.

The XML file conforms to the XML schema definition that supports import of user. This schema addresses the complete user attributes, for more information, see [XML Schema Definition for bulk import of users](#) on page 408.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export user job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

When you import the same file to a new system, you must provide the password for users with any administrative role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with any administrative role fails, if the password is not provided.

To import users with any administrative role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

For **Partial Merge/Replace** import type, if you do not specify the password, the existing password remains.



You can export user data in bulk from System Manager web console.

### Bulk export users directory

The bulk export users zip files are stored in the `/var/avaya/bulkadministration/export/` directory. The total file size of exported zip files is monitored as per the value of the **max\_bulk\_export\_files\_directory\_size\_allowed** property in the `$MGMT_HOME/bulkadministration/exportutility/config/bulkexportconfig.properties` directory. The default file size for bulk export user is 1-GB. You can change the file size value for bulk export user to maximum 2-GB.

The system runs the check for the total size of the files in the `/var/avaya/bulkadministration/export/` directory on a daily basis. If the file size is greater than **max\_bulk\_export\_files\_directory\_size\_allowed**, the system automatically deletes the oldest files to make the size less than or equal to **max\_bulk\_export\_files\_directory\_size\_allowed**.

#### \* Note:

If there is only one file in `/var/avaya/bulkadministration/export/`, the system does not delete the file.

## Exporting users in bulk from web console

### About this task

With bulk export you can export the delta of users for a specified period of time. Delta users are the added, updated, or deleted users for the specified period of time. This feature is useful for performing bulk export of the entire System Manager user database that can be used with the external applications. This feature enables you to export only the users that have changed during the defined interval.

#### ! Important:

- The system runs the export users job that you schedule only once. To export users the next time, you must create a new export job by using this procedure. You cannot reschedule an existing export job.
- Increasing number of users per file in bulk export configuration beyond verified default limit consumes system resources. It results in degrading system performance and can cause system crash.

### Procedure

1. On the System Manager web console, click **Users > User Management**.
2. On the User management page, click one of the following:
  - **More Actions > Export All Users** to export user records for all users.
  - **More Actions > Export Selected Users** to export user records for the users that you select.

#### \* Note:

- If you select specific users from the list and click **Export All**, the system exports the records of all users instead of the selected records.

- If you provide the criteria in **Advanced Search** and click **Export All**, the system exports only the records that match the criteria.

- **More Actions > Export Delta Users** to export the delta of users for a specified period of time.

The system displays the Export Users page.

3. In the Export File Type Options section, in **Select Export File Types**, click **Xml**, **Excel** or both.

 **Note:**

Select at least one option. If you do not select a file type, and click **Export**, the export operation does not start. The page displays the message `Export File Type/Types Not Selected`. Select `Export File Types Xml` or `Excel` or `Both`.

If you select only **Excel**, the system automatically clears the **Contacts** check box in **User Attribute Options** because excel file does not support importing and exporting user contacts. The page also displays a message `Excel file does not support contacts` beside the **Contacts** check box.

4. **(Optional)** In the User Attribute Options section, select one or more check boxes to export contacts and specific communication profiles.

By default, the system exports basic attributes, communication profiles, and contacts.

For more information, see “Export Users field descriptions”.

5. In the Delta Period Options section, from **Select the delta period**, select the delta period to generate the file for the delta of users.

The Delta Period Options section is available only if you select the **Export Delta Users** option.

For more information, see “Export Users field descriptions”.

For example, if you select the delta period as **One Week**, schedule the job with the **Run immediately** option, and export file type as both XML and Excel, then the exported zip file contains the following:

- An `XML` file with added or updated users in last one week.
- An `Excel` file with added or updated users in last one week.
- A `deleted users .txt` file only if there are any permanently deleted users in the specified delta period.

6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

For more information, see “Export Users field descriptions”.

 **Important:**

The export users job that you schedule runs only once. To export users the next time, you must create a new export job by using this procedure. You cannot reschedule an existing export job.

7. Click **Export** to complete the export operation.

The system exports the user data to the XML and Excel file.

8. To view the data, in the **Export List** section, click the link in the **Download File** column.

To use the exported excel file for operations such as reimporting, while exporting users from the Export Users page, clear the **Contacts** check box in User Attribute Options. Excel export or import operations does not support export or import of contacts that are associated with the user.

### Related links

[Bulk export of users](#) on page 382

[List of XML Schema Definitions and sample XMLs for bulk import](#) on page 408

[exportUpmGlobalsettings.sh command](#) on page 403

[Attribute details defined in Import user XSD](#) on page 524

[Attribute details defined in Delete User XSD](#) on page 535

[Attribute details defined in the CM Endpoint profile XSD](#) on page 536

[Attribute details defined in the Messaging communication profile XSD](#) on page 565

[Attribute details defined in the Session Manager communication profile XSD](#) on page 574

[Export Users field descriptions](#) on page 386

[Downloading the Excel template file](#) on page 381

[Microsoft Excel data link error](#) on page 375

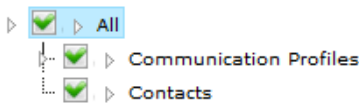
[Bulk importing of users](#) on page 379

## Export Users field descriptions

### Export File Type Options

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Export File Types | <p>The file type to which you want to export the users. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Xml</b></li> <li>• <b>Excel</b></li> <li>• <b>Both</b>. You can select <b>Xml</b> and <b>Excel</b>.</li> </ul> <p> <b>Note:</b></p> <p>Select at least one option. If you do not select a file type, and click <b>Export</b>, the export operation does not start. The page displays the message <code>Export File Type/Types Not Selected</code>. Select <code>Export File Types Xml</code> or <code>Excel</code> or <code>Both</code>.</p> <p>If you select only <b>Excel</b>, the system automatically clears the <b>Contacts</b> check box in <b>User Attribute Options</b> because excel file does not support importing and exporting user contacts. The page also displays a message <code>Excel file does not support contacts</code> beside the <b>Contacts</b> check box.</p> |

## User Attribute Options

| Name                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>User attribute options that an export administrator can choose to export for an export job.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>All:</b> The system exports all user attributes that includes all communications profiles and contacts. The default is <b>All</b>.</li> <li>• <b>Communications Profiles:</b> The export administrators can select communication profiles they want to export. For example : If the administrator selects all check boxes and clears the Session Manager profile check box, the system exports users with all data except the Session Manager communication profile attributes.</li> <li>• <b>Contacts:</b> The system exports all contacts. The system does not exports contacts if the check box is clear.</li> </ul> <p> <b>Note:</b></p> <p>When you select the <b>Contacts</b> check box, the system exports the contacts of users only to an XML file. The system does not support exporting contacts to an Excel file.</p> <p> <b>Important:</b></p> <p>If the exported file is used to import by using the replace option, the import operation replaces the existing user data from the system with user data in the exported file that might be incomplete because of the filter applied during the export.</p> |

## Delta Period options

The Delta Period Options section is available only if you select the **Export Delta Users** option.

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select the delta period</b> | <p>Following are the delta period options:</p> <ul style="list-style-type: none"> <li>• <b>One Day:</b> is exact past one day from current system date and time for run immediately or exact past one day from scheduled job time.</li> <li>• <b>One Week:</b> is exact past one week from current system date and time for run immediately or exact past one week from scheduled job time.</li> <li>• <b>One Month:</b> is exact past one month from current system date and time for run immediately or exact past one month from scheduled job time.</li> </ul> <p> <b>Note:</b></p> <p>The system creates the <code>XML</code> and <code>Excel</code> file even if there are no added or updated users in the specified delta period. If there are no added or updated users in the specified delta period then the <code>XML</code> and <code>Excel</code> files contain zero users data. However, the system creates the <code>.txt</code> file only if there are any permanently deleted users in the specified delta period.</p> |

## Schedule

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Job</b> | <p>The settings to configure the schedule of the job. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Run immediately</b>: To run the export job immediately.</li> <li>• <b>Schedule later</b>: To run the job at the specified date and time.</li> </ul> <p> <b>Note:</b></p> <p>If you select the <b>Export All Users</b> or <b>Export Delta Users</b> option, and select the <b>Schedule Job</b> as <b>Schedule later</b>, the system displays the <b>Recurrence</b> and <b>Range</b> fields.</p> |
| <b>Date</b>         | <p>The date when you must run the export job. The date format is mm dd yyyy. You can use the calendar icon to choose a date.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Time</b>         | <p>The time of running the export job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Time Zone</b>    | <p>The time zone of your region.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recurrence</b> | <p>Following are the options:</p> <ul style="list-style-type: none"> <li>• <b>Execute task one time only:</b> The job is executed only once at the specified scheduled start time.</li> <li>• <b>Tasks are repeated:</b> The options are <b>Daily</b>, <b>Weekly</b>, and <b>Monthly</b>. The job is repeated as per the selection.</li> </ul> <p> <b>Note:</b></p> <p>If you select the <b>Tasks are repeated</b>, the system enables the <b>Range</b> field.</p> <p> <b>Note:</b></p> <p>The delta period selected for the <b>Export Delta Users</b> option for scheduled or recurring jobs will consider the exact delta period past to the exact start date and time of execution of the scheduled jobs.</p> <p>For example, if a delta export job is scheduled to run on December 17, 2017 at 2:00 p.m. with the delta period of <b>One Day</b>, then the delta of users is identified from December 16, 2017 from 2.00 p.m.</p> <p>For recurrence jobs, if a job is configured to run multiple times then the last exported zip file with the name <code>&lt;Scheduled Job Name&gt;.zip</code> will be available on the Export Users page for download. However, the previously exported zip files will be stored in the <code>/var/avaya/bulkadministration/export/</code> directory with the name <code>&lt;Scheduled Job_Date_time_In_UTC&gt;.zip</code>.</p> <p>Where <i>Date_time_In_UTC</i> is the date and time in UTC when the file was last-updated or created in the last run of the job.</p> <p>For example, if the admin started a recurring job at 18 Dec 2017 14:32:26 UTC to run for say 3 recurrences daily then after the completion of all 3 recurrences there will be 3 files available in the <code>/var/avaya/bulkadministration/export/</code> directory with following names: <code>users_1503066729239_18-Dec-2017_14:32:37_UTC.zip</code>, <code>users_1503066729239_19-Dec-2017_14:32:32_UTC.zip</code>, and <code>users_1503066729239.zip</code>.</p> |
| <b>Range</b>      | <p>Following are the options:</p> <ul style="list-style-type: none"> <li>• <b>No End Date:</b> The job has no end date and executed as per the selection in the <b>Tasks are repeated</b> field.</li> <li>• <b>End After Occurrences:</b> The job is executed as per the selection in the <b>Tasks are repeated</b> field for the number of occurrences specified in <b>End After Occurrences</b>.</li> <li>• <b>End By Date:</b> The job is executed and the recurrence ends when the end date is reached.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Button        | Description                                                                |
|---------------|----------------------------------------------------------------------------|
| <b>Export</b> | Exports or schedules the export job based on the option that you selected. |

## Export List

| Name                    | Description                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b> | The option to select a job.                                                                                                                                                                                                                                                                                                                               |
| <b>Start Time</b>       | The date and time when the job was scheduled.                                                                                                                                                                                                                                                                                                             |
| <b>Status</b>           | The status of the job. The options are: <ul style="list-style-type: none"> <li>• PENDING EXECUTION: The job is in queue.</li> <li>• RUNNING: The job execution is in progress.</li> <li>• SUCCESSFUL: The job execution is completed.</li> <li>• INTERRUPTED: The job execution is cancelled.</li> <li>• FAILED: The job execution has failed.</li> </ul> |
| <b>Scheduled Job</b>    | A key to the Scheduler page. You can cancel the job from the Scheduler page.                                                                                                                                                                                                                                                                              |
| <b>% Complete</b>       | The job completion status in percentage.                                                                                                                                                                                                                                                                                                                  |
| <b>User Records</b>     | The total number of user records that are marked for export.                                                                                                                                                                                                                                                                                              |
| <b>Failed Records</b>   | The number of user records that failed to export.                                                                                                                                                                                                                                                                                                         |
| <b>Download File</b>    | The link to download the zip file that contains XML and Excel files.                                                                                                                                                                                                                                                                                      |

| Button              | Description                                      |
|---------------------|--------------------------------------------------|
| <b>View</b>         | Displays the details of the selected job.        |
| <b>Stop</b>         | Stops the export operation for the selected job. |
| <b>Delete</b>       | Deletes the job that you selected.               |
| <b>Refresh</b>      | Refreshes the job details.                       |
| <b>Select: All</b>  | Selects all the jobs from the list.              |
| <b>Select: None</b> | Clears the check box selections.                 |
| <b>Previous</b>     | Displays jobs in the previous page.              |
| <b>Next</b>         | Displays jobs in the next page.                  |
| <b>Done</b>         | Returns to the User Management page.             |

## Configuring the maximum file size for automatically removing the exported zip files from the bulk export users directory

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.



2. From the `$MGMT_HOME/bulkadministration/exportutility/config` location, open the `bulkexportconfig.properties` file.
3. In the `bulkexportconfig.properties` file, change the value of **max\_bulk\_export\_files\_directory\_size\_allowed**.

Do not enter the decimal value for the file size. The default file size for bulk export user is 1-GB. You can change the file size value for bulk export user to maximum 2-GB.

## Configuration options for bulk import of users

You can bulk import only the selected user attributes data for one or more users existing in the database. The XML file must conform to XML schema definition, for more information, see [XML Schema Definition for partial import of users](#) on page 423. For a sample XML file for import of user, see [Sample XML for partial import of users](#) on page 425.

The following configuration options are available for import of users:

- Abort or continue the import process when the import user operation encounters first error in the user input file.
- Perform one of the following import types:
  - The partial import type. Helps import of users with specific user attributes.
  - The complete import type. Helps import of users with all user attributes.
- If a matching record already exists, you can:
  - Replace the users in the database with the new users from the file you imported. For example, you can replace the existing contact list for a user with a new contact list.
  - Merge the user attributes data from the imported file to the existing data. For example, you can add a new contact in the list of contacts for the user and update the name of the user.
  - Delete the user records from the database that match the records in the input XML file.
- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of user records in the input file
  - Total number of user records with warnings in the input file
  - Total number of user records that fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.

- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

## Bulk importing of partial user attributes for a user

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.

Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.

3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:
  - XML
  - Excel

#### **Note:**

Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release`. Use the Excel template that you downloaded or exported from the current System Manager release.

4. Select one of the following error configuration options:
  - **Abort on first error**
  - **Continue processing other records**
5. Select **Partial** as the import type.
6. Select one of the following options to handle matching records:
  - To replace the existing attribute data of a matching user in the database with the new data from the imported file, click **Replace**.
  - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
7. To run the job, in the Job Schedule section, select one of the following:
  - To import the users immediately, click **Run immediately**.
  - To import the users at a specified time, click **Schedule later**, and set date and time.
8. Click **Import**.

### Related links

[About bulk import of users](#) on page 377

[List of XML Schema Definitions and sample XMLs for bulk import](#) on page 408

[Attribute details defined in Import user XSD](#) on page 524

[Attribute details defined in Delete User XSD](#) on page 535

[Attribute details defined in the CM Endpoint profile XSD](#) on page 536

[Attribute details defined in the Messaging communication profile XSD](#) on page 565

[Attribute details defined in the Session Manager communication profile XSD](#) on page 574

[Configuration options for bulk import of users](#) on page 391

## Making exported user data compatible for partial user import

Use this section to update user attributes partially. XML file format contains the user records that System Manager exports. You must update selected user attributes in the exported XML file and then import the XML file. You require this procedure because export users generate XML file conforming to this XML Schema Definition. For more information, see [XML Schema Definition for bulk import of users](#) on page 408. Partial import type uses a different XML schema definition, for more information, see [XML Schema Definition for partial import of user attributes](#) on page 423.

### Before you begin

Export the users in bulk and generate the XML file.

### About this task

For partial import of users, make the following changes in the user export XML file. You can generate the XML file by exporting users in bulk.

### Procedure

#### 1. Perform the following steps:

##### a. Locate the following content in the generated XML file:

```
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
```

##### b. Modify `tns:users` to `tns:deltaUserList`.

##### c. Remove `tns="http://xml.avaya.com/schema/import"`.

##### d. Modify `ns4="http://xml.avaya.com/schema/deltaImport"` to `tns="http://xml.avaya.com/schema/deltaImport"`

##### e. Modify `xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">` to `xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">`

After you modify the XML file as instructed in Step b through Step e, the content in Step a changes to:

```
<tns:deltaUserList xmlns:ns3="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">
```

2. Replace all instances of:

- `<tns:user>` with `<tns:userDelta>`
- `</tns:user>` with `</tns:userDelta>`
- `<tns:users>` with `<tns:deltaUserList>`
- `</tns:users>` with `</tns:deltaUserList>`

### Next steps

You can now make the updates in the XML file and import the changes to update the user attributes in the database.

## About Bulk Import Encryption utility

System Manager Import User supports import of encrypted user password field and the plain text Communication Profile password field into the database. For importing a user XML file with encrypted password, System Manager provides BulkImportEncryptionUtil, a utility tool that encrypts the “userPassword” and “commPassword” fields in the user import input file.

The utility tool takes an XML file with plaintext password field values as input. This utility encrypts the password fields and generates an XML file with encrypted password field. You can use the XML file to import user.

BulkImportEncryptionUtil is a standalone Java program. You can run the utility on any machine that has Java installed on it.

## Encrypting passwords in user import file using BulkImportEncryptionUtil running on Windows

### Before you begin

JDK 1.6 is installed on your computer. If the computer does not have JDK 1.6 installed, use the <http://java.sun.com/javase/downloads/index.jsp> URL to download JDK 1.6.

### Procedure

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

The `um_bulkimport-encryptUtil.zip` file contains the following files:

- `um_bulkimport-encryptUtil.jar`
- `log4j.jar` and script files
- `um_bulkimport-encryptUtil.bat`
- `um_bulkimport-encryptUtil.sh`
- `Readme.txt`

2. At the command prompt, type `um_bulkimport-encryptUtil.bat <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:

- `import|deltaimport` specifies whether the input XML file has data for complete import or partial import. For complete import, this option value is `import` and for partial import this option value is `deltaimport`.
- `xmlfilename` is the name of the XML file with complete path of the XML file that contains the data for importing the users data
- `basenamespaceprefix` is the namespace prefix in the input XML file. In the following example, `tns` is the value for the `basenamespaceprefix` parameter.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
```

- `deltanamespaceprefix` is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, the `deltanamespaceprefix` value is `delta` and `basenamespaceprefix` value is `tns`.

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList
xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

#### Related links

[About Bulk Import Encryption utility](#) on page 394

## Encrypting passwords in user import file using BulkImportEncryptionUtil running on Linux

### Before you begin

Install JDK 1.6 on your computer. If the computer does not have JDK 1.6 installed, use the <http://java.sun.com/javase/downloads/index.jsp> URL to download JDK 1.6.

### Procedure

1. Extract the contents of the `um_bulkimport-encryptUtil.zip` file from `$MGMT_HOME/upm/utilities` into a local folder.

The `um_bulkimport-encryptUtil.zip` file contains the following files:

- `um_bulkimport-encryptUtil.jar`
- `log4j.jar` and script files
- `um_bulkimport-encryptUtil.bat`
- `um_bulkimport-encryptUtil.sh`

- Readme.txt
- 2. At the command prompt, type `um_bulkimport-encryptUtil.sh <import|deltaimport> <xmlfilename> <basenamespaceprefix> <deltanamespaceprefix>`, where:
  - *import* | *deltaimport* specifies whether the input XML file has data for complete import or partial import. For complete import, this option value is *import* and for partial import this option value is *deltaimport*.
  - *xmlfilename* is the name of the XML file with complete path of the XML file that contains the data for importing the users data
  - *basenamespaceprefix* is the namespace prefix in the input XML file. In the following example, *tns* is the value for the *basenamespaceprefix* parameter.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
```

- *deltanamespaceprefix* is the namespace prefix given in the partial import file. Specify this parameter if you are performing a partial import. In the following example, the *deltanamespaceprefix* value is *delta* and *basenamespaceprefix* value is *tns*.

```
<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList
xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd ">
```

## Related links

[About Bulk Import Encryption utility](#) on page 394

## Import user considerations

- If the *comprofileset* has associated *handlelist* or *commprofilelist*, you cannot merge or replace *commprofileset* attributes name and *lsprimary*.

To move *handlelist* and *commprofilelist* from one *commprofileset* to another, perform the following:

1. Perform Replace - Import file with no *commprofileset*.
  2. Perform Update (merge/replace) - Import file with the new *commprofileset* with associated *handlelist* and *commprofiles*.
- For security reasons, you do not export the **Password** fields in the XML file.

When you import the same file to a new system, you must provide the password for users with any administrative role. For security reasons, the system does not export the **Password** fields to the XML file. Therefore, import of users with any administrative role fails, if the password is not provided.

To import users with any administrative role, in the XML file for the users, add the following XML tag after the `<username>` tag:

```
<userPassword> provide password for user </userPassword>
```

For **Partial Merge/Replace** import type, if you do not specify the password, the existing password remains.

- To enhance the performance of a file with large user records, split the file into smaller file sizes. For example, you can split a user import file of 15 Kb into three files of 5 Kb each. To speed up the import process, schedule three import jobs in parallel. System Manager has the ability to process multiple files concurrently.

## Scheduling a user import job

System Manager supports scheduling of bulk import jobs from the System Manager console. You can schedule a job to run immediately or at a later time.

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.

Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.

3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:
  - XML
  - Excel

#### **Note:**

Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release`. Use the Excel template that you downloaded or exported from the current System Manager release.

4. Select one of the following error configuration options:
  - **Abort on first error**
  - **Continue processing other records**
5. Select one of the following import options:
  - To skip users in the import file that match the existing user records in the database, click **Skip**.
  - To replace the users in the database with new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.

If you select Excel file type, the system does not display the replace option

- To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
- To delete the user records in the database that match the records in the imported file, click **Delete**.

 **Note:**

For import by using Excel, the system deletes the user records permanently.

6. In the Job Schedule section:

a. Click **Schedule later**.

To run the user import job immediately, click **Run immediately**. When you select this option, the fields related to scheduling become unavailable.

b. In the **Date** field, type the date.

You can use the calendar icon to select a date.

c. In the **Time** field, type the time in the HH:MM:SS format.

d. In the **Time Zone** field, type the time zone.

7. Click **Import**.

The page displays the scheduled job in the Manage Jobs section.

## Aborting a user import job on first error

System Manager supports the following error configurations:

- Abort on first error: Aborts import of the user records when the import user operation encounters the first error in the import file containing the user records.
- Continue processing other records: Imports the next user record even if the import user operation encounters an error while importing a user record.

### About this task

The user import process may encounter errors at the time of importing of users. Use this feature to configure actions when you encounter the first error. You can choose to abort the user import process or continue the import process.

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.

Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.

3. On the Import users page, in the **Select Import File Type** field, select one of the following file types:
  - XML



- Excel

**\* Note:**

Use the Excel template that System Manager supports. If you use an unsupported template, the system displays a message `<file_name>.xlsx file is not a valid excel template for the current System Manager release.` Use the Excel template that you downloaded or exported from the current System Manager release.

4. Click **Abort on first error** to choose error configuration options.
5. Select one of the following import options:
  - To skip users in the import file that match the existing user records in the database, click **Skip**.
  - To replace the users in the database with new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.  
If you select Excel file type, the system does not display the replace option
  - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
  - To delete the user records in the database that match the records in the imported file, click **Delete**.

**\* Note:**

For import by using Excel, the system deletes the user records permanently.

6. Choose or enter the appropriate information for remaining fields.
7. Click **Import**.

## Canceling a user import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.  
Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.
3. On the Import Users page, select the job from the table in the Manage Jobs section.
4. Click **Cancel job**.

## Deleting a user import job

System Manager supports deleting of jobs. **Delete job** option removes the job information from the database.

## About this task

You can delete a job only when the status of the job is SUCCESSFUL. To interrupt a job that is running or pending, use the **Cancel job** option.

## Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.  
Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.
3. On the Import Users page, select the job to delete from the table in the Manage Jobs section.
4. Click **Delete job**.

## Viewing a user import job on the Scheduler page

You can view an import job on the Scheduler Web page. You can perform all operations on a job that Scheduler supports from the Scheduler page.

## Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.  
Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.
3. On the Import Users page, select a job from the table in the Manage Jobs section.
4. Click the link displayed in the **Job Name** column.

The Scheduler page displays the details of the job. You can perform operations on the job that the Scheduler supports for the job.

## Viewing the details of a user import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time
- Selected error configuration option
- Selected import type option
- Selected import option
- Job end time

- Job status
- Import file name
- Total number of user records in the import file
- Total number of user records successfully imported
- Total number of user records that failed to import
- Total number of warnings
- Percentage complete status

### About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Users**.  
  
Also, to gain access to **Import users**, from the System Manager web console, click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Users**.
3. On the Import Users page, select a job to view from the table in the Manage Jobs section.
4. Click **View job**.

The Job Detail page displays the details of the selected job.

## Bulk import of global user settings

You can use the *Import Global Settings* functionality to import global settings in bulk from an XML file. The XML file must conform to XML schema definition, for more information, see [XML Schema Definition for bulk import of global setting records](#) on page 508. For sample XML file for import global settings, see [Sample XML for bulk import of global setting records](#) on page 514.

You can perform the following tasks with Import Global Settings:

- Abort or continue the import process when the import operation encounters first error in the global user settings input file.
- Skip importing the global user settings records that already exist in the database. Use this option to import new global user settings records and retain the existing users.
- Update and merge the global user settings attributes data from the imported file to the existing data in the attributes.
- Replace all the global user settings records in the database with the global user settings records from the imported file.
- Delete the global setting records from the database that match the records in the input XML file.

- Schedule the bulk import job.
- View the details of an import job:
  - Job scheduled time
  - Job end time
  - Job status
  - Job completion status in percentage
  - Total number of global settings records in the input file
  - The number of global settings records with warnings in the input file
  - The number of global settings records fail to import in the input file
  - The link to the Scheduler user interface
- Cancel or delete an import job.
- View logs of records that fail to import and require manual intervention.
- Download failed records in an XML file. The XML file conforms to XML schema definition. You can modify the failed records and import the records again to the database.

To add and update (Merge and Replace) global settings use [XML Schema Definition for bulk import of global setting records](#) on page 508.

To delete bulk global settings, use the XML schema definition for global settings delete, see [XML Schema Definition for bulk deletion of global setting records](#) on page 518. For a sample XML conforming to delete bulk global settings XML schema definition, see [Sample XML for bulk deletion of users](#) on page 428.

## Bulk importing the global user settings

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.
3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

Also, you can click **Browse** to select a file.
4. Select one of the following error configuration options:
  - **Abort on first error**
  - **Continue processing other records**

5. Select one of the import options:
  - **Skip**
  - **Replace**
  - **Merge**
  - **Delete**
6. In the **Job Schedule** section, select one of the following options:
  - To run the import job immediately, click **Run immediately**.
  - To run the import job at a later time, click **Schedule later** and set the date and time.
7. Click **Import**.

### Related links

[About bulk import of users](#) on page 377

[List of XML Schema Definitions and sample XMLs for bulk import](#) on page 408

[Bulk import of global user settings](#) on page 401

## Bulk export of global user settings

In System Manager, you can export global settings in bulk from the System Manager database.

You can export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

The Export User process creates an archive file containing one or more XML files. While exporting the global settings records, if the number of exported records exceed the limit of records that an XML file can hold, the system creates multiple XML files. The system packages the XML files in a zip file.

The XML file conforms to the XML schema definition that supports import of global settings. This schema addresses the complete global settings attributes. For more information, see [XML Schema Definition for bulk import of global setting records](#) on page 508.

The system generates the XML file on the System Manager server. You can specify the location of the file you want to export while running the Export User job.

You can schedule an export global settings job. The job parameter provides an option to specify the schedule time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.

You can export user data in bulk from System Manager web console.

## exportUpmGlobalsettings.sh command

Use the **exportUpmGlobalsettings** command to export global settings from the System Manager database.

## Syntax

```
exportUpmGlobalsettings.sh -f globalSettingExport-r-d -s -e-t
```

- f** The prefix of the file name for the file that you require to export.
- r** The number of records per file.
- d** The location of the file that you want to export.
- s** The start index of record.
- e** The number of records you want to export.
- t** The job scheduling time in the YYYY:MM:DD:HH:MM:SS format. If you do not specify this parameter, the present job runs immediately.
- o** The global settings export filter. The default is 0. You can set one of the following values for the global settings export filter:
  - **0** No Filter. 0 is considered as the start index value.
  - **1** System Default Type filter
  - **2** Enforced users filter
  - **3** System Rule Type filter
  - **4** System ACL Entry Type filter
  - **5** Shared Address filter
  - **6** Public Contact filter

## Scheduling a global user settings import job

### About this task

System Manager supports scheduling of bulk import jobs from the System Manager web console. With the scheduling utility, you can schedule an import job to run immediately or at a later time.

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.

3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

Also, you can click **Browse** to select a file.

4. Select one of the following error configuration options:
  - **Abort on first error**
  - **Continue processing other records**
5. Select one of the import options:
  - **Skip**
  - **Replace**
  - **Merge**
  - **Delete**
6. In the **Job Schedule** section:
  - a. Click **Schedule later**.
 

To run the import job immediately, click **Run immediately**. After you select this option, the fields related to scheduling become unavailable.
  - b. In the **Date** field, type the date.
 

You can use the calendar icon to select a date.
  - c. In the **Time** field, type time in the HH:MM:SS format.
  - d. In the **Time Zone** field, select a time zone.
7. Click **Import**.
 

The system displays the scheduled job in the Manage Jobs section.

## Viewing details of a global user settings import job

You can view the following details of an import job:

- Job name
- Job scheduled by
- Job scheduled start time
- Job end time
- Job status
- Import file name
- Total number of user records in the import file
- Total number of user records successfully imported
- Total number of user records that failed to import
- Percentage complete status

### About this task

You can view the error message for each user record that fails to import. You can download the failed user records in an XML file format. You can modify the XML file and import the file again.

## Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **View job**.

The Job Detail page displays the details of the selected job.

## Viewing a global user settings import job on the Scheduler page

### About this task

You can view and perform all operations on an import job that the scheduler supports from the Scheduler page.

### Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Job section.
4. Click the link in the **Job Name** column.

The Scheduler page displays the details of the job.

## Aborting a global user settings import job on first error

System Manager supports the following error configurations:

- Abort on first error. Aborts importing of the global settings records when the import global settings operation encounters the first error in the import file that contains the global settings records.
- Continue processing other records. Imports the next global settings record even if the import operation encounters an error while importing a global settings record.

### About this task

You can abort an import process when the import process encounters the first error in the input file while processing the global user settings records.



## Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.

3. On the Import Global Settings page, enter the complete path of the file in the **Select file** field.

Also, you can click **Browse** to select a file.

4. Select **Abort on first error** as the error configuration option.
5. Select one of the import options:
  - **Skip**
  - **Replace**
  - **Merge**
  - **Delete**
6. Choose or enter the appropriate information for the remaining fields.
7. Click **Import**.

## Deleting a global user settings import job

System Manager supports deletion of an import job. The **Delete job** option removes the job information from the database. You can delete a job only when the job is in the *SUCCESSFUL* state.

To interrupt a job that is running or pending, use the **Cancel job** option.

## Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **Delete Job**.

## Canceling a global user settings import job

You can cancel a job only when the job is in the PENDING EXECUTION or RUNNING state.

## Procedure

1. On the System Manager web console, click **Services > Bulk Import and Export**.
2. Click **Import > User Management > Global Settings**.

To gain access to **Import Global Settings**, from the System Manager Console you can also click **Users > User Management**. Click **Manage Users** and select **More Actions > Import Global Settings**.

3. On the Import Global Settings page, select a job from the table in the Manage Jobs section.
4. Click **Cancel job**.

## List of XML Schema Definitions and sample XMLs for bulk import

The section contains the XML Schema Definition and sample XML snippets for bulk import of users, global setting records, elements, endpoint profiles, Messaging profiles, CS 1000 profiles, IP Office profiles, agent profiles, Session Manager profiles, Presence profiles, Avaya Breeze® platform, Work Assignment, Conferencing, Avaya Messaging, and Avaya Meetings Server profiles.

### \* Note:

You cannot use the following characters as is in the XML file. To use the characters in the import of XML files, make the following modifications:

- Less-than character (<) as &lt;
- Ampersand character (&) as &amp;
- Greater-than character (>) as &gt;
- Double-quote character (") as &quot;
- Apostrophe or single-quote character (') as &apos;

If you copy the XML schema from the document, take care of the line breaks.

### XML Schema Definition for bulk import of users

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/import" version="2.0">
 <xs:element name="secureStore" type="tns:xmlSecureStore"/>
 <xs:element name="user" type="tns:xmlUser"/>
 <xs:element name="users">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="secureStore" type="tns:xmlSecureStore" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="user" type="tns:xmlUser" minOccurs="0"
maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 <xs:complexType name="xmlUser">
 <xs:sequence>
 <xs:element name="UserOrganizationDetails"
type="tns:UserOrganizationDetailsType"
maxOccurs="1" minOccurs="0" />
 </xs:sequence>
 </xs:complexType>
</xs:schema>
```

```

<xs:element name="UserProvisionRules" minOccurs="0">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="UserProvisionRuleName" type="xs:string"
minOccurs="0" maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="authenticationType" type="xs:string"
 minOccurs="1" maxOccurs="1" />
<xs:element name="description" type="xs:string"
 minOccurs="0" />
<xs:element name="displayName" type="xs:string"
 minOccurs="0" />
<xs:element name="displayNameAscii" type="xs:string"
 minOccurs="0" />
<xs:element name="dn" type="xs:string" minOccurs="0" />
<xs:element name="isDuplicatedLoginAllowed"
 type="xs:boolean" minOccurs="0" />
<xs:element name="isEnabled" type="xs:boolean" minOccurs="0"
 maxOccurs="1" />
<xs:element name="isVirtualUser" type="xs:boolean"
 minOccurs="0" />
<xs:element name="givenName" type="xs:string" minOccurs="1"
 maxOccurs="1" />
<xs:element name="givenNameAscii" type="xs:string" minOccurs="0"
 maxOccurs="1" />
<xs:element name="honorific" type="xs:string" minOccurs="0" />
<xs:element name="loginName" minOccurs="1" maxOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="128" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>
<xs:element name="newLoginName" minOccurs="0" maxOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="128" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>
<xs:element name="employeeNo" type="xs:string"
 minOccurs="0" maxOccurs="1">
</xs:element>
<xs:element name="department" type="xs:string" minOccurs="0"
 maxOccurs="1">
</xs:element>
<xs:element name="organization" type="xs:string"
 minOccurs="0" maxOccurs="1">
</xs:element>
<xs:element name="middleName" type="xs:string"
 minOccurs="0" />
<xs:element name="managerName" type="xs:string"
 minOccurs="0" />
<xs:element name="preferredGivenName" type="xs:string"
 minOccurs="0" />
<xs:element name="preferredLanguage" type="xs:string"
 minOccurs="0" />
<xs:element name="source" type="xs:string" minOccurs="0"
 maxOccurs="1" />
<xs:element name="sourceUserKey" type="xs:string"
 minOccurs="0" maxOccurs="1" />
<xs:element name="status" type="xs:string" minOccurs="0" />
<xs:element name="suffix" type="xs:string" minOccurs="0" />

```

```

 <xs:element name="surname" type="xs:string" minOccurs="1"
 maxOccurs="1" />
 <xs:element name="surnameAscii" type="xs:string" minOccurs="0"
 maxOccurs="1" />
 <xs:element name="timeZone" type="xs:string" minOccurs="0" />
 <xs:element name="title" type="xs:string" minOccurs="0" />
 <xs:element name="userName" type="xs:string" minOccurs="0"
 maxOccurs="1" />
 <xs:element name="userPassword" type="xs:string"
 minOccurs="0" />
 <xs:element name="commPassword" type="xs:string"
 minOccurs="0" />
 <xs:element name="userType" type="xs:string" minOccurs="0"
 maxOccurs="unbounded" />
 <xs:element name="roles" minOccurs="0">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="role" type="xs:string"
 minOccurs="0" maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 <xs:element name="localizedNames" type="tns:xmlLocalizedNames" minOccurs="0"
 maxOccurs="1"></xs:element>
 <xs:element name="address" type="tns:xmlAddress"
 minOccurs="0" maxOccurs="unbounded" />
 <xs:element name="securityIdentity"
 type="tns:xmlSecurityIdentity" minOccurs="0" maxOccurs="unbounded" />
 <!-- Contact list Entries -->
 <xs:element name="ownedContactLists" minOccurs="0"
 maxOccurs="1">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="contactList"
 type="tns:xmlContactList" maxOccurs="1" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 <xs:element name="ownedContacts" minOccurs="0">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="contact" type="tns:xmlContact"
 maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 <!-- Presence ACL User Entries -->
 <xs:element name="presenceUserDefault"
 type="tns:xmlPresUserDefaultType" minOccurs="0" />
 <xs:element name="presenceUserACL"
 type="tns:xmlPresUserACLEntryType" minOccurs="0"
 maxOccurs="unbounded" />
 <xs:element name="presenceUserCLDefault"
 type="tns:xmlPresUserCLDefaultType" minOccurs="0" maxOccurs="1" />
 <xs:element name="commProfileSet"
 type="tns:xmlCommProfileSetType" minOccurs="0"
 maxOccurs="unbounded" />

 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlSecurityIdentity">
 <xs:sequence>
 <xs:element name="identity" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="realm" type="xs:string" minOccurs="0"/>
 <xs:element name="type" type="xs:string" minOccurs="1" maxOccurs="1"/>
 </xs:sequence>

```

```

 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlPresInfoTypeAccessType">
 <xs:sequence>
 <xs:element name="infoType" type="tns:xmlPresInfoTypeType" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="access" type="xs:string" minOccurs="0" maxOccurs="1"/>
 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlPresACRuleType">
 <xs:sequence>
 <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlPresUserDefaultType">
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType"/>
 </xs:complexContent>
 </xs:complexType>
 <xs:complexType name="xmlPresUserCLDefaultType">
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType"/>
 </xs:complexContent>
 </xs:complexType>
 <xs:complexType name="xmlPresUserACLEntryType">
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType">
 <xs:sequence>
 <xs:choice>
minOccurs="0"/>
 <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
 <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
 </xs:choice>
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
 </xs:complexType>
 <xs:complexType name="xmlPresInfoTypeType">
 <xs:sequence>
 <xs:element name="label" type="xs:string" maxOccurs="1"/>
 <xs:element name="filter" type="xs:string" maxOccurs="1"/>
 <xs:element name="specFlags" type="xs:string" minOccurs="0"/>
 </xs:sequence>
 </xs:complexType>
 <!-- Contact List entries -->
 <xs:complexType name="xmlContactList">
 <xs:sequence>
 <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="description" type="xs:string" minOccurs="0"/>
 <xs:element name="isPublic" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
 <xs:element name="members" type="tns:xmlContactListMember" minOccurs="0"
maxOccurs="unbounded"/>
 <xs:element name="contactListType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlContactListMember">
 <xs:sequence>
 <xs:choice>
 <xs:sequence>
 <xs:element name="memberContact" type="xs:string" minOccurs="0"/>
 <xs:element name="speedDialContactAddress"
type="tns:xmlContactAddress" minOccurs="0"/>

```

```

 </xs:sequence>
 <xs:sequence>
 <xs:element name="memberUser" type="xs:string" minOccurs="0"/>
 <xs:element name="speedDialHandle" type="tns:xmlHandle"
minOccurs="0"/>
 </xs:sequence>
 </xs:choice>
 <xs:element name="isFavorite" type="xs:boolean" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="isSpeedDial" type="xs:boolean" minOccurs="1"/>
 <xs:element name="speedDialEntry" type="xs:int" minOccurs="0"/>
 <xs:element name="isPresenceBuddy" type="xs:boolean" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="label" type="xs:string" minOccurs="0"/>
 <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
 <xs:element name="description" type="xs:string" minOccurs="0"/>
 <xs:element name="priorityLevel" type="xs:int" minOccurs="0"/>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContactAddress">
 <xs:sequence>
 <xs:element name="address" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="altLabel" type="xs:string" minOccurs="0"/>
 <xs:element name="contactCategory" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="contactType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="label" type="xs:string" minOccurs="0"/>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlAddress">
 <xs:sequence>
 <xs:element name="addressType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="building" type="xs:string" minOccurs="0"/>
 <xs:element name="localityName" type="xs:string" minOccurs="0"/>
 <xs:element name="postalCode" type="xs:string" minOccurs="0"/>
 <!-- Additional Attribute Support - The attribute room will be mapped to
cubical.-->
 <xs:element name="room" type="xs:string" minOccurs="0"/>
 <xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
 <xs:element name="country" type="xs:string" minOccurs="0"/>
 <xs:element name="street" type="xs:string" minOccurs="0"/>
 <!-- Additional Attribute Support -->
 <xs:element name="businessphone" type="xs:string" minOccurs="0"/>
 <xs:element name="otherbusinessphone" type="xs:string" minOccurs="0"/>
 <xs:element name="fax" type="xs:string" minOccurs="0"/>
 <xs:element name="homephone" type="xs:string" minOccurs="0"/>
 <xs:element name="otherhomephone" type="xs:string" minOccurs="0"/>
 <xs:element name="mobilephone" type="xs:string" minOccurs="0"/>
 <xs:element name="othermobilephone" type="xs:string" minOccurs="0"/>
 <xs:element name="pager" type="xs:string" minOccurs="0"/>
 <xs:element name="pager2" type="xs:string" minOccurs="0"/>
 <!-- Additional Attribute Support - End -->
 <xs:element name="postalAddress" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="1024"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="isPrivate" type="xs:boolean" minOccurs="0"/>
 </xs:sequence>
</xs:complexType>

```

```

 <xs:complexType name="xmlContact">
 <xs:sequence>
 <xs:element name="company" type="xs:string" minOccurs="0"/>
 <xs:element name="description" type="xs:string" minOccurs="0"/>
 <xs:element name="displayName" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="displayNameAscii" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="dn" type="xs:string" minOccurs="0"/>
 <xs:element name="givenName" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="givenNameAscii" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="initials" type="xs:string" minOccurs="0"/>
 <xs:element name="middleName" type="xs:string" minOccurs="0"/>
 <xs:element name="preferredGivenName" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
 <xs:element name="isPublic" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
 <xs:element name="source" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="sourceUserKey" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="suffix" type="xs:string" minOccurs="0"/>
 <xs:element name="surname" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="surnameAscii" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="title" type="xs:string" minOccurs="0"/>
 <xs:element name="ContactAddress" type="tns:xmlContactAddress"
minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="addresses" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlHandle">
 <xs:sequence>
 <xs:element name="handleName" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="handleType" type="xs:string" minOccurs="1" maxOccurs="1"/>
 <xs:element name="handleSubType" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="domainName" type="xs:string" minOccurs="0" maxOccurs="1"/>
 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlCommProfileType">
 <xs:sequence>
 <xs:element name="commProfileType" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="commProfileSubType" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="jobId" type="xs:string" minOccurs="0" maxOccurs="1"/>
 </xs:sequence>
 </xs:complexType>
 <xs:complexType name="xmlCommProfileSetType">
 <xs:sequence>
 <xs:element name="commProfileSetName" type="xs:string" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="isPrimary" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
 <xs:element name="handleList" minOccurs="0">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="handle" type="tns:xmlHandle"
maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 <xs:element name="commProfileList" minOccurs="0">
 <xs:complexType>

```

```

 <xs:sequence>
 <xs:element name="commProfile" type="tns:xmlCommProfileType"
maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="ForgeinCommProfileType">
 <xs:complexContent>
 <xs:extension base="ext:xmlCommProfileType">
 <xs:sequence>
 <xs:element name="csEncryptionKeyId" type="xs:long" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="servicePassword" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 <xs:element name="serviceData" type="xs:string" minOccurs="0"
maxOccurs="1"/>
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlSecureStore">
 <xs:sequence>
 <xs:element name="secureStoreData" type="xs:base64Binary" minOccurs="1"
maxOccurs="1"/>
 <xs:element name="passwordEncrypted" type="xs:boolean"/>
 </xs:sequence>
</xs:complexType>

 <xs:complexType name="xmlLocalizedName">
 <xs:sequence>
 <xs:element name="locale" type="xs:string" minOccurs="1"
maxOccurs="1">
 </xs:element>
 <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"></
xs:element>
 </xs:sequence>
 </xs:complexType>

 <xs:complexType name="xmLocalizedNames">
 <xs:sequence>
 <xs:element name="localizedName" type="tns:xmlLocalizedName" minOccurs="0"
maxOccurs="7"></xs:element>
 </xs:sequence>
 </xs:complexType>

 <xs:complexType name="UserOrganizationDetailsType">
 <xs:sequence>
 <xs:element name="tenant" maxOccurs="1" minOccurs="1">
 <xs:complexType>
 <xs:attribute name="name" type="xs:string" use="required"/>
 <xs:attribute name="createTenantIfNotAlreadyPresent"
type="xs:boolean"
use="required"/>
 </xs:complexType>
 </xs:element>
 <xs:element name="organizationUnitLevelOne" type="xs:string"
maxOccurs="1" minOccurs="0">
 </xs:element>
 <xs:element name="organizationUnitLevelTwo" type="xs:string"
maxOccurs="1" minOccurs="0">
 </xs:element>
 <xs:element name="organizationUnitLevelThree" type="xs:string"
maxOccurs="1" minOccurs="0">

```



```

 </xs:element>
 </xs:sequence>
 </xs:complexType>
 </xs:schema>

```

### Sample XML for bulk import of users with minimal attributes

```

<?xml version="1.0" encoding="UTF-8"?>
 <!-- Root Element 'Users' represent collection of user (containing 1 or
 more users)-->
 <tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/
 2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
 userimport.xsd" >

 <tns:user>
 <authenticationType>Basic</authenticationType>
 <givenName>John</givenName>
 <loginName>jmiller@avaya.com</loginName>
 <surname>Miller</surname>
 <userPassword>mypassword</userPassword>
 </tns:user>
 </tns:users>

```

### Sample XML for bulk import of users with all attributes

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- Root Element 'Users' represent collection of user (containing 1 or more
users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd">
<!-- authenticationType: This defines the type of authentication that this user
will undergo at runtime to obtain access to the system.
Possible Values: BASIC,ENTERPRISE
---description:A text description of the user. Human readable description of
this user instance.
---displayName:The localized name of a user to be used when displaying. It
will typically be the localized full name. This value may be provisioned
from the users enterprise directory entry. If it does not exist,
synchronization rules can be used to populate it for other fields
e.g. Surname, GivenName, or LoginName.
---displayNameAscii:This corresponds to the
Console attribute-Endpoint Display Name.
The full text name of the user represented in ASCII. It is used to support
display (e.g. endpoints) that cannot handle localized text
---dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with
an associated value in the form of attribute=value, normally expressed in a
UTF-8 string format.The dn can be used to identify the user and may be used
for authentication subject mapping. Note the dn is changeable.
---isDuplicatedLoginAllowed:A boolean indicator showing whether this user is
allowed a duplicate concurrent logins.A true stipulates that the user is
allow to have duplicate logins. Default value is true.
---isEnabled:A boolean indicator showing whether or not the user is active.
Users with AuthenticationType equals Basic will fail if this value is false.
This attribute can be used to disable access between login attempts.
A running sessions login will not be revocable. Alternatively the
administrator can always modify the password to disable the user from
logging in. A true stipulates this is an active user, a false used for a
disabled user. Default value is false.
---isVirtualUser:A boolean indicator showing whether or not the record is being
used for a non-human entity such as an application, service, software agent,
etc. This is to be used where the entity will behave as a user and needs to
have subset of the user profile populated. If the entity does not behave as

```

a user and has a different trust relationship e.g. a trust certificate it should not be treated as a virtual user. A virtual user can represent an Avaya or external non-human entity. This attribute is provided as a convenience to track such accounts. A true stipulates this is a virtual user, a false is used for human users. Default value is false.

---givenName:The first name of the user.

---honorific:The personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to PersonalTitle.

---loginName:This is the unique system login name given to the user. It can take the form of username@domain or just username. This may vary across customers. It can be used to help provision default user handles in the CSHandle table. The username is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc3986.

.....userinfo / loginname = \*( unreserved / pct-encoded / sub-delims / ":" )  
 where <p>unreserved = ALPHA / DIGIT / "-" / "." / "\_" / "~"

.....pct-encoded = "%" HEXDIG HEXDIG  
 sub-delims = "!" / "\$" / "&" / "'" / "(" / ")" / "\*" / "+" / "," / ";" / "="

---employeeNo:Employee number of user.

---department:Department of employee.

---organization:Organization of employee.

---middleName:The middle name of the user.

---managerName:Text name of the users manager. This is a free formed field and does not require the users manager to also be a user of the solution. This attribute was requested to support reporting needs.

---preferredGivenName:The preferred first name of the user.

---preferredLanguage:The individuals preferred written or spoken language. Values will conform to rfc4646 and the reader should refer to rfc4646 for syntax. This format uses the ISO standard Language ISO639 and region ISO3166 codes. In the absence of a value the clients locale should be used, if no value is set, en-US should be defaulted.

---source:Free format text field that identifies the entity that created this user record. The format of this field will be either a IP Address/Port or a name representing an enterprise LDAP or Avaya.

---sourceUserKey:The key of the user from the source system. If the source is an Enterprise Active Directory server, this value will be the objectGUID.

---status:This information is to help manage provisioning activities such as correcting or completing the provisioning of a user instance. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED).  
 Possible Values: AUTHPENDING;PENDINGAUTHZ;PROVISIONED

---suffix:The text appended to a name e.g. Jr., III.

---surname:The users last name, also called the family name.

---timeZone:The preferred time zone of the user.  
 For example: (-12:0)International Date Line West.

---title:The job function of a person in their organizational context.

---userName:This is the username portion of the loginName field. It is an alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with \_ . - % ! ~ \* ( ) = + \$ , ; and ? special characters are supported.

This is the rfc2798 uid attribute.

---userPassword:The encrypted password for this users account. A null password is used when the user is authenticated by the enterprise such as with a separate source such as the enterprise LDAP.

---commPassword:The encrypted subscriber or communication password with which the user logs can use to authentication with on to any CommProfile SIP and non SIP. This attribute is meant to be a shared across different communication profiles and thus different communication services.

---userType:This enumerates the possible primary user application types. A User can be associated with multiple user types. Possible values are ADMINISTRATOR; COMMUNICATION USER; AGENT; SUPERVISOR; RESIDENT EXPERT; SERVICE TECHNICIAN; LOBBY PHONE

---roles:Text name of a role. This value needs to pre-exist in SMGR DB

---localizedNames:localized name of user.

```

---address:The address of the user.
---securityIdentity:The SecurityIdentity is used to hold any additional
identities for a user that can be used for authentication such as their
loginName, Kerberos account name, or their X509 certificate name.
---ownedContactLists:It is a collection of internal or external contacts.
ContactList is owned by a specific user and has a name that a unique name
within the context of its owner.
---ownedContacts:It represents a non Avaya application user (external) contact.
Contacts can be collected together along with User entities into a contact
list. Contacts can be created by an administrator or an end user.
---presenceUserDefault:These are personal rules that are set by presentities
to define how much presence information can be shown to watchers that are
not explicitly mentioned in an ACL. There may be one User Default rule per
presentity (User), or none.
---presenceUserACL:These are personal rules defined by presentities themselves
on who can monitor their presence information. There may be several entries
in the list for a given presentity, each entry corresponding to one watcher.
---presenceUserCLDefault:This is a personal rule that is set by presentities
to define how much presence information can be shown to watchers that belong
to the userss contact list. There may be one User Contact List Default rule
per presentity (Person) or none.
---commProfileSet:A user will have a default commprofile set.A commprofile set
can exist without any handles or commprofiles referencing it. I.e. you can
create a commprofile set without needing to also create either a handle or
a commprofile.A commprofile set can contain multiple commprofiles, but only
one of each specific type. This is enforced by having the CSCCommProfile
uniqueness constraint include type, cs_commpfile_set_id.
-->
<tns:user>
 <authenticationType>BASIC</authenticationType>
 <description>this is description</description>
 <displayName> John Miller</displayName>
 <displayNameAscii></displayNameAscii>
 <dn>dc=acme,dc=org</dn>
 <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>John</givenName>
 <honorific>Mr</honorific>
 <loginName>jmiller@avaya.com</loginName>
 <employeeNo>20060441</employeeNo>
 <department>UC</department>
 <organization>GCS</organization>
 <middleName></middleName>
 <managerName>Jay Smith</managerName>
 <preferredGivenName>John</preferredGivenName>
 <preferredLanguage>English</preferredLanguage>
 <source>LDAP</source>
 <sourceUserKey>18966</sourceUserKey>
 <status>AUTHPENDING</status>
 <suffix>Mr</suffix>
 <surname>Miller</surname>
 <timeZone>(-12:0) International Date Line West</timeZone>
 <title>Mr</title>
 <userName>jmiller</userName>
 <userPassword>password</userPassword>
 <commPassword>mycommPassword</commPassword>
 <userType>ADMINISTRATOR</userType>
 <roles>
 <role>End-User</role>
 </roles>
 <localizedNames>
 <localizedName>
 <locale>English</locale>
 <name>John</name>

```

```

</localizedName>
</localizedNames>
<!--addressType:Specifies the role of the address. Examples: Home, business.
---name:The Name property defines the unique label by which the address is
 known. Default format for user specific address should include user name
 place address type.
---building:The name or other designation of a structure
---localityName:The name of a locality, such as a city, county or other
 geographic region.
---postalCode:A code used by postal services to route mail to a destination.
 In the United States this is the zip code.
---room:Name or designation of a room.
---stateOrProvince:The full name of a state or province.
---country:A country.
---street:The physical address of the object such as an address for package
 delivery
---postalAddress:A free formed text area for the complete physical delivery
 address. It may be used in place of the specific fields in this table.
---isPrivate:A boolean indicator to specify if this address could be shared
 across multiple users.True is private, false is sharable. Default is false.
-->
<address>
 <addressType>OFFICE</addressType>
 <name>Avaya Office</name>
 <building>building 11</building>
 <localityName>Magarpatta</localityName>
 <postalCode>411028</postalCode>
 <room>room 502</room>
 <stateOrProvince>Maharashtra</stateOrProvince>
 <country>India</country>
 <street>street</street>
 <postalAddress></postalAddress>
 <isPrivate>true</isPrivate>
</address>
<!--
---SecurityIdentity:Represents the possible external identities that a user
 may have for the purpose of authentication. The type and format of an
 identity depends on the external Identity Provider and can include
 X.509 certificates or Kerberos user accounts
---identity:The unique external identity of the user. This is a free text
 field and no format is enforced. The format will depend on the identity
 type. Kerberos user account can take the form of: username@domainName
 e.g. jsmith@acme.org
---realm:The name of the security domain that this identity is valid in.
---type:The text representation of the type of identity.
 Possible values are: principalname,X509 and Kerberos
-->
<securityIdentity>
 <identity>jmiller@acme.org </identity>
 <realm>acme</realm>
 <type>principalname</type>
</securityIdentity>
<!--
---ContactList:The ContactList is a collection of personal or public groups
 containing external contacts and/or Avaya users.
---name:The text name of the list. This in the context of the owner must be
 unique.
---description:A free text description of this member.
---isPublic:Defines if the contact is public or personal. Default = false.
---members:Represents the list of users or contacts that belong to contact list
---contactListType:Specifies the type categorizing this list.
-->
<ownedContactLists>
 <contactList>
 <name>MycontactList</name>

```

```

<description>This is my contactList</description>
<isPublic>>false</isPublic>
<!--
---memberContact:This represents the name of the Contact.
 A ContactListMember can either be a Contact or User
---speedDialContactAddress:A Contact Address added as a favorite entry
---memberUser:This represents the loginname of the User.
 A ContactListMember can either be a Contact or User
---speedDialHandle:A handle added as a favorite entry
---isFavorite:A boolean indicator that reflects whether this contact is
 a favorite entry. If true, the value of entryindex would show which
 position to place this entry in any display.
---isSpeedDial:Each contact list member can also be flagged as a
 favorite (a.k.a. speed dial)
---speedDialEntry:For either a presence buddy or favorite entry, a
 specific communication address to use can be pointed to.
---isPresenceBuddy:Each contact list member can also be flagged as a
 presence buddy
---label:A free text short word or phrase for classifying this contact
 list member.
---altLabel:A free text short word or phrase for classifying this
 contact.This is similar to label, but it is used to store alternate
 language representations.
---description:A free text description of this member.
-->
<members>
 <memberContact>Phil Bath</memberContact>
 <speedDialContactAddress>
 <address>+44-1234568</address>
 <altLabel>Phone</altLabel>
 <contactCategory>OFFICE</contactCategory>
 <contactType>PHONE</contactType>
 <label>Phone</label>
 </speedDialContactAddress>
 <isFavorite>true</isFavorite>
 <isSpeedDial>true</isSpeedDial>
 <speedDialEntry>1234</speedDialEntry>
 <isPresence>Buddytrue</isPresenceBuddy>
 <label>My Contact in Dublin office</label>
 <altLabel>Phone Number for contacting Denver office</altLabel>
 <description>Contact Details</description>
 <priorityLevel>0</priorityLevel>
</members>
<contactListType>CONTACTCENTER</contactListType>
</contactList>
</ownedContactLists>
<!--
---Contact:An entity that represents a non Avaya application user (external)
 contact. Contacts can be collected together along with User entities into
 a contact list. Contacts can be created by an administrator or an end
 user. Contacts have name attributes, and owner, and can be public or
 personal. A contact also includes one or more contact addresses that can
 be used for establishing an interaction with the contact. Contacts can be
 designated as being a users presence buddy or added as a favorite entry
 For example, speed dial.
---company:The organization that the contact belongs to.
---description:A free text field containing human readable text providing
 information on this entry.
---displayName:The localized name of a contact to be used when displaying.
 It will typically be the localized full name. This value may be provisioned
 from the users enterprise directory entry. If it does not exist,
 synchronization rules can be used to populate it for other fields
 e.g. Surname, GivenName, or LoginName.
---displayNameAscii:The full text name of the contact represented in ASCII.
 It is used to support display (e.g. endpoints) that cannot handle

```

```

 localized text.
---dn:The distinguished name of the user. The DN is a sequence of relative
 distinguished names (RDN) connected by commas. An RDN is an attribute
 with an associated value in the form of attribute=value, normally expressed
 in a UTF-8 string format.The dn can be used to uniquely identify this
 record. Note the dn is changeable.
---givenName:The first name of the contact.
---initials:Initials of the contact
---middleName:The middle name of the contact.
---preferredGivenName:The nick name of the contact.
---preferredLanguage:The individuals preferred written or spoken language.
 Values will conform to rfc4646 and the reader should refer to rfc4646
 for syntax.This format uses the ISO standard Language ISO639 and region
 ISO3166 codes. In the absence of a value the clients locale should be
 used, if no value is set, en-US should be defaulted.
---isPublic:Defines if the contact is public or personal. Default = false.
---source:Free format text field that identifies the entity that created
 this user record. The format of this field will be either a
 IP Address/Port or a name representing an enterprise LDAP or Avaya.
---sourceUserKey:The key of the user from the source system. If the source is
 an Enterprise Active Directory server, this value will be the objectGUID.
---suffix:The text appended to a name e.g. Jr., III.
---surname:The users last name, also called the family name.
---title:The job function of a person in their organizational context.
 Examples: supervisor, manager
---ContactAddress:Represents a contacts address.
---addresses:A fully qualified URI for interacting with this contact. Any
 addresses added to this table should contain a qualifier e.g. sip, sips,
 tel, mailto. The address should be syntactically valid based on the
 qualifier. It must be possible to add via the GUI and Interface.
 The application must do validation.
-->
<ownedContacts>
 <contact>
 <company>ABC</company>
 <description>Company ABC description</description>
 <displayName>Phil Bath</displayName>
 <displayNameAscii></displayNameAscii>
 <dn>dc=acme,dc=org</dn>
 <givenName>John</givenName>
 <initials>Mr</initials>
 <middleName>M</middleName>
 <preferredGivenName>Phil</preferredGivenName>
 <preferredLanguage>English</preferredLanguage>
 <isPublic>>false</isPublic>
 <source>ldap</source>
 <sourceUserKey>123546</sourceUserKey>
 <suffix>Jr.</suffix>
 <surname>Bath</surname>
 <title>Manager</title>
 <!--
 ---type:The value reflecting the type of handle this is. Possible
 values are username, e164, and privatesubsystem
 ---category:The value representing a further qualification to the contact
 address. Possible values include Office, Home, Mobile.
 ---handle:This is the name given to the user to allow communication to
 be established with the user. It is an alphanumeric value that must
 comply with the userinfo related portion of a URI as described in rfc2396.
 However, it is further restricted as ASCII characters with only the
 + prefix to signify this is an E.164 handle and _ and . special
 characters supported.The handle and type together are unique within a
 specific domain. Note, the handle plus domain can be used to construct
 a users Address of Record.
 ---label:A free text description for classifying this contact.

```

```

 ---altLabel:A free text description for classifying this contact. This is
 similar to ContactLabel, but it is used to store alternate language
 representations.
 -->
<ContactAddress>
 <address>+44-1234568</address>
 <altLabel>Phone</altLabel>
 <contactCategory>OFFICE</contactCategory>
 <contactType>PHONE</contactType>
 <label>Phone</label>
</ContactAddress>
<addresses>
<!--
 ---addressType:The unique text name of the address type.
 Possible values are: Home, business.
 ---name: The Name property defines the unique label by which the address
 is known. Default format for user specific address should include
 user name place address type.
 ---building:The name or other designation of a structure.
 ---localityName:The name of a locality, such as a city, county or other
 geographic region.
 ---postalCode:A code used by postal services to route mail to a
 destination. In the United States this is the zip code.
 ---room:Name or designation of a room.
 ---stateOrProvince:The full name of a state or province.
 ---country:A country.
 ---street:The physical address of the object such as an address for
 package delivery
 ---postalAddress:A free formed text area for the complete physical delivery
 address. It may be used in place of the specific fields in this table.
-->

 <addressType>office</addressType>
 <name>Phil Bath</name>
 <building>building A</building>
 <localityName>Magarpatta</localityName>
 <postalCode>411048</postalCode>
 <room>room 123</room>
 <stateOrProvince>MH</stateOrProvince>
 <country>India</country>
 <street>Hadapsar</street>
 <isPrivate>true</isPrivate>

</addresses>
</contact>
</ownedContacts>
<!--
 ---PresUserDefault:These are personal rules that are set by presentities to
 define how much presence information can be shown to watchers that are
 not explicitly mentioned in an ACL. There may be one User Default rule
 per presentity (User), or none.presentity (User), or none.
 ---label:A unique string that names this info type (e.g. Telephony Presence)
 ---filter:Internal definition of which part of presence information is
 covered by this info type. The value of this field should be treated
 as opaque string; it is maintained and used only by Presence services.
 ---specFlags:This field is empty for regular info types, but for special
 info types it contains a comma separated list of keywords that identify
 these types. In this version only FULL that represents full presence
 information is supported.
-->
 <presenceUserDefault>
 <infoTypeAccess>
 <infoType>
 <label>Telephony Presence</label>
 <filter>filter</filter>

```



```

 <specFlags>FULL</specFlags>
 </infoType>
 <access>BLOCK</access>
</infoTypeAccess>
</presenceUserDefault>
<!--
 ---UserACLEntry:These are personal rules defined by presentities
 themselves on who can monitor their presence information. There may be
 several entries in the list for a given presentity, each entry
 corresponding to one watcher.
 ---label:A unique string that names this info type (e.g. Telephony Presence).
 ---filter:Internal definition of which part of presence information is
 covered by this info type. The value of this field should be treated
 as opaque string; it is maintained and used only by Presence services.
 ---specFlags:This field is empty for regular info types, but for special info
 types it contains a comma separated list of keywords that identify these
 types. In this version only FULL that represents full presence
 information is supported.
-->
 <presenceUserACL>
 <infoTypeAccess>
 <infoType>
 <label>ALL</label>
 <filter>filter</filter>
 <specFlags>FULL</specFlags>
 </infoType>
 <access>BLOCK</access>
 </infoTypeAccess>
 <watcherLoginName>admin</watcherLoginName>
 </presenceUserACL>
 <!--
 PresUserCLDefault:This is a personal rule that is set by presentities
 to define how much presence information can be shown to watchers
 that belong to the users contact list. There may be one User
 Contact List Default rule per presentity (Person) or none.
 -->
 <presenceUserCLDefault>
 <infoTypeAccess>
 <infoType>
 <label>Telephony</label>
 <filter>filter</filter>
 <specFlags>FULL</specFlags>
 </infoType>
 <access>BLOCK</access>
 </infoTypeAccess>
 </presenceUserCLDefault>
<!--
 commProfileSet:A user will have a default commprofile set.A commprofile
 set can exist without any handles or commprofiles referencing it. I.e.
 you can create a commprofile set without needing to also create either
 a handle or a commprofile.A commprofile set can contain multiple
 commprofiles, but only one of each specific type. This is enforced by
 having the CommProfile uniqueness constraint include type,
 commprofile_set_id.
 ---HandleName:This is the name given to the user to allow communication to
 be established with the user. It is an alphanumeric value that must comply
 with the userinfo related portion of a URI as described in rfc2396.
 However,it is further restricted as ASCII characters with only
 the + prefix to signify this is an E.164 handle and _ and .
 special characters supported. Note, the handle plus domain can be used
 to construct a users Address of Record.
 ---handleType:The value reflecting the type of handle this is. Possible values
 are sip,smtp,ibm,and xmpp.
 ---handleSubType:This is an additional qualify on the handle type to help
 specify which private subsystem this handle belongs to.Possible values are
 e164,username,msrtc,googletalk,jabber,ibmsametime,lotousnotes,msexchageo.
-->

```



```

 ---domainName:The text name of the domain.
-->
<commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <handleList>
 <handle>
 <handleName>sip:abc@yahoo.com</handleName>
 <handleType>sip</handleType>
 <handleSubType>msrtc</handleSubType>
 </handle>
 </handleList>
 <!--The below is extended communication profile-->
<!--
 <commProfileList>
 <commProfile xsi:type="ns3:SessionManagerCommProfXML" xmlns:ns3="http://
xml.avaya.com/schema/import_sessionmanager">
 <commProfileType>SessionManager</commProfileType>
 <ns3:primarySM>SIP Entity 1</ns3:primarySM>
 <ns3:secondarySM>SIP Entity 2</ns3:secondarySM>
 <ns3:survivabilityServer>SIP Entity 2</ns3:survivabilityServer>
 <ns3:terminationAppSequence>AppSeq1</ns3:terminationAppSequence>
 <ns3:originationAppSequence>AppSeq2</ns3:originationAppSequence>
 <ns3:homeLocation>Denver</ns3:homeLocation>
 <ns3:confFactorySet>Factory Set 1</ns3:confFactorySet>
 </commProfile>
 </commProfileList>
-->
</commProfileSet>

</tns:user>
</tns:users>

```

## XML Schema Definition for partial import of users

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<xs:schema xmlns:delta="http://xml.avaya.com/schema/deltaImport" xmlns:base="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/deltaImport" version="1.0">

 <xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

 <xs:element name="userDelta" type="delta:xmlUserDelta"/>
 <xs:element name="deltaUserList" type="delta:xmlDeltaUserList"/>

 <xs:complexType name="xmlDeltaUserList">
 <xs:sequence>
 <xs:element name="secureStore" type="base:xmlSecureStore"></xs:element>
 <xs:element name="userDelta" type="delta:xmlUserDelta" minOccurs="0"
maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>

 <xs:complexType name="xmlUserDelta">
 <xs:sequence>
 <xs:element name="authenticationType"
type="xs:string" minOccurs="0" maxOccurs="1" />
 <xs:element name="description" type="xs:string"
minOccurs="0" />
 <xs:element name="displayName" type="xs:string"
minOccurs="0" />
 </xs:sequence>
 </xs:complexType>

```

```

<xs:element name="displayNameAscii" type="xs:string"
 minOccurs="0" />
<xs:element name="dn" type="xs:string" minOccurs="0" />
<xs:element name="isDuplicatedLoginAllowed"
 type="xs:boolean" minOccurs="0" />
<xs:element name="isEnabled" type="xs:boolean" minOccurs="0"
 maxOccurs="1" />
<xs:element name="isVirtualUser" type="xs:boolean"
 minOccurs="0" />
<xs:element name="givenName" type="xs:string" maxOccurs="1"
 minOccurs="0" />
<xs:element name="honorific" type="xs:string" minOccurs="0" />
<xs:element name="loginName" type="xs:string" maxOccurs="1"
 minOccurs="1" />
<xs:element name="middleName" type="xs:string"
 minOccurs="0" />
<xs:element name="managerName" type="xs:string"
 minOccurs="0" />
<xs:element name="preferredGivenName" type="xs:string"
 minOccurs="0" />
<xs:element name="preferredLanguage" type="xs:string"
 minOccurs="0" />
<xs:element name="source" type="xs:string" minOccurs="0"
 maxOccurs="1" />
<xs:element name="sourceUserKey" type="xs:string"
 minOccurs="0" maxOccurs="1" />
<xs:element name="status" type="xs:string"
 minOccurs="0" />
<xs:element name="suffix" type="xs:string" minOccurs="0" />
<xs:element name="surname" type="xs:string" minOccurs="0"
 maxOccurs="1" />
<xs:element name="timeZone" type="xs:string" minOccurs="0" />
<xs:element name="title" type="xs:string" minOccurs="0" />
<xs:element name="userName" type="xs:string" maxOccurs="1"
 minOccurs="0" />
<xs:element name="userPassword" type="xs:string"
 minOccurs="0" />
<xs:element name="commPassword" type="xs:string"
 minOccurs="0" />
<xs:element name="userType" type="xs:string"
 minOccurs="0" maxOccurs="unbounded" />
<xs:element name="roles" minOccurs="0">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="role" type="xs:string"
 minOccurs="0" maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="address" type="base:xmlAddress"
 minOccurs="0" maxOccurs="unbounded" />
<xs:element name="securityIdentity"
 type="base:xmlSecurityIdentity" minOccurs="0" maxOccurs="unbounded" />
<!-- Contact list Entries -->
<xs:element name="ownedContactLists" minOccurs="0"
 maxOccurs="1">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="contactList"
 type="base:xmlContactList" maxOccurs="1" />
 </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="ownedContacts" minOccurs="0">
 <xs:complexType>

```

```

 <xs:sequence>
 <xs:element name="contact" type="base:xmlContact"
 maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
</xs:element>
<!-- Presence ACL User Entries -->
<xs:element name="presenceUserDefault"
 type="base:xmlPresUserDefaultType" minOccurs="0" />
<xs:element name="presenceUserACL"
 type="base:xmlPresUserACLEntryType" minOccurs="0"
 maxOccurs="unbounded" />
<xs:element name="presenceUserCLDefault"
 type="base:xmlPresUserCLDefaultType" minOccurs="0" maxOccurs="1" />
<xs:element name="commProfileSet"
 type="base:xmlCommProfileSetType" maxOccurs="unbounded" minOccurs="0">
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

### Sample XML for partial import of users

```

<?xml version="1.0" encoding="UTF-8"?>
<delta:deltaUserList xmlns:delta="http://xml.avaya.com/schema/deltaImport"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport
userdeltaimport.xsd">
 <delta:userDelta>
 <authenticationType>ENTERPRISE</authenticationType>
 <description>this is description</description>
 <displayName>John Miller</displayName>
 <displayNameAscii></displayNameAscii>
 <dn>dc=acme,dc=org</dn>
 <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>true</isVirtualUser>
 <givenName>John</givenName>
 <honorific>Mr</honorific>
 <loginName>jmiller@avaya.com</loginName>
 <middleName></middleName>
 <managerName>Jay Smith</managerName>
 <preferredGivenName>John</preferredGivenName>
 <preferredLanguage>English</preferredLanguage>
 <source>LDAP</source>
 <sourceUserKey>18966</sourceUserKey>
 <status>AUTHPENDING</status>
 <suffix>Mr</suffix>
 <surname>Miller</surname>
 <timeZone>(-12:00) International Date Line West</timeZone>
 <title>Mr</title>
 <userName>jmiller</userName>
 <commPassword>mycommPassword</commPassword>
 <userType>ADMINISTRATOR</userType>
 <roles>
 <role>End-User</role>
 </roles>
 <address>
 <addressType>OFFICE</addressType>
 <name>Avaya Office</name>
 <building>building 11</building>
 <localityName>Magarpatta</localityName>
 <postalCode>411028</postalCode>
 <room>room 502</room>
 </address>
 </delta:userDelta>
</delta:deltaUserList>

```

```

 <stateOrProvince>Maharashtra</stateOrProvince>
 <country>India</country>
 <street>street</street>
 <postalAddress></postalAddress>
 <isPrivate>true</isPrivate>
 </address>
 <securityIdentity>
 <identity>jmiller@acme.org </identity>
 <realm>acme</realm>
 <type>principalname</type>
 </securityIdentity>
 <ownedContactLists>
 <contactList>
 <name>MycontactList</name>
 <description>This is my contactList</description>
 <isPublic>>false</isPublic>
 <members>
 <memberContact>Phil Bath</memberContact>
 <speedDialContactAddress>
 <address>+44-1234568</address>
 <altLabel>Phone</altLabel>
 <contactCategory>OFFICE</contactCategory>
 <contactType>PHONE</contactType>
 <label>Phone</label>
 </speedDialContactAddress>
 <isFavorite>true</isFavorite>
 <isSpeedDial>true</isSpeedDial>
 <speedDialEntry>1234</speedDialEntry>
 <isPresenceBuddy>true</isPresenceBuddy>
 <label>My Contact in Dublin office</label>
 <altLabel>Phone Number for contacting Denver office</altLabel>
 <description>Contact Details</description>
 <priorityLevel>0</priorityLevel>
 </members>
 <contactListType>CONTACTCENTER</contactListType>
 </contactList>
 </ownedContactLists>
 <ownedContacts>
 <contact>
 <company>ABC</company>
 <description>Company ABC description</description>
 <displayName>Phil Bath</displayName>
 <displayNameAscii></displayNameAscii>
 <dn>dc=acme,dc=org</dn>
 <givenName>John</givenName>
 <initials>Mr</initials>
 <middleName>M</middleName>
 <preferredGivenName>Phil</preferredGivenName>
 <preferredLanguage>English</preferredLanguage>
 <isPublic>>false</isPublic>
 <source>ldap</source>
 <sourceUserKey>123546</sourceUserKey>
 <suffix>Jr.</suffix>
 <surname>Bath</surname>
 <title>Manager</title>
 <ContactAddress>
 <address>+44-1234568</address>
 <altLabel>Phone</altLabel>
 <contactCategory>OFFICE</contactCategory>
 <contactType>PHONE</contactType>
 <label>Phone</label>
 </ContactAddress>
 <addresses>
 <addressType>office</addressType>
 <name>Phil Bath</name>

```

```

 <building>building A</building>
 <localityName>Magarpatta</localityName>
 <postalCode>411048</postalCode>
 <room>room 123</room>
 <stateOrProvince>MH</stateOrProvince>
 <country>India</country>
 <street>Hadapsar</street>
 <isPrivate>true</isPrivate>
 </addresses>
</contact>
</ownedContacts>
<presenceUserDefault>
 <infoTypeAccess>
 <infoType>
 <label>Telephony Presence</label>
 <filter>filter</filter>
 <specFlags>FULL</specFlags>
 </infoType>
 <access>BLOCK</access>
 </infoTypeAccess>
</presenceUserDefault>
<presenceUserACL>
 <infoTypeAccess>
 <infoType>
 <label>ALL</label>
 <filter>filter</filter>
 <specFlags>FULL</specFlags>
 </infoType>
 <access>BLOCK</access>
 </infoTypeAccess>
 <watcherLoginName>admin</watcherLoginName>
</presenceUserACL>
<presenceUserCLDefault>
 <infoTypeAccess>
 <infoType>
 <label>Telephony</label>
 <filter>filter</filter>
 <specFlags>FULL</specFlags>
 </infoType>
 <access>BLOCK</access>
 </infoTypeAccess>
</presenceUserCLDefault>
</delta:userDelta>
</delta:deltaUserList>

```

## XML Schema Definition for bulk deletion of users

```

<xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete" targetNamespace="http://
xml.avaya.com/schema/bulkdelete"
 elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/
2001/XMLSchema" >

 <xs:element name="user" type="tns:xmlUserDelete" />
 <xs:element name="deleteType" type="tns:xmlDeleteType" />

 <xs:element name="deleteUsers">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="deleteType" type="tns:xmlDeleteType" maxOccurs="1"
minOccurs="1"/>
 <xs:element minOccurs="1" maxOccurs="unbounded" name="user"
type="tns:xmlUserDelete" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>

```

```

 </xs:complexType>
 </xs:element>

 <xs:complexType name="xmlUserDelete">
 <xs:sequence>
 <xs:element name="loginName" minOccurs="1" maxOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="128"/></xs:maxLength>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="id" type="xs:string" maxOccurs="1" minOccurs="0"/></
xs:element>
 </xs:sequence>
 </xs:complexType>

 <xs:simpleType name="xmlDeleteType">
 <xs:restriction base="xs:string"></xs:restriction>
 </xs:simpleType>
</xs:schema>

```

### Sample XML for bulk deletion of users

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteUsers xmlns:tns="http://xml.avaya.com/schema/bulkdelete" xmlns:ns2="http://
xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/bulkdelete
UserProfileSchemaDefinitionForBulkDelete.xsd">
<tns:deleteType>permanent</tns:deleteType>
 <tns:user>
 <tns:loginName>jmiller@avaya.com</tns:loginName>
 </tns:user>
 <tns:user>
 <tns:loginName>david@avaya.com</tns:loginName>
 </tns:user>
</tns:deleteUsers>

```

### XML Schema Definition for bulk import of elements

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.avaya.com/rtts"
 xmlns="http://www.avaya.com/rtts"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified" attributeFormDefault="unqualified">

 <!-- <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"> -->
 <xs:element name="RTSElements">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="ApplicationSystems" minOccurs="0"
 maxOccurs="unbounded">
 <xs:annotation>
 <xs:documentation>
 Application System Types
 </xs:documentation>
 </xs:annotation>
 <xs:complexType>
 <xs:sequence>
 <xs:element name="ApplicationSystem"
 type="ApplicationSystem" maxOccurs="unbounded">
 </xs:element>
 </xs:sequence>
 </xs:element>
 </xs:sequence>
 </xs:complexType>
 </xs:element>

```

```

 </xs:complexType>
 </xs:element>
 <xs:element name="ApplicationSystemAssigns"
 minOccurs="0" maxOccurs="unbounded">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="Source" type="Source"
 minOccurs="1" maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 </xs:sequence>
 </xs:complexType>
</xs:element>

<xs:complexType name="ApplicationSystem">
 <xs:annotation>
 <xs:documentation></xs:documentation>
 </xs:annotation>

 <xs:sequence>
 <xs:element name="Host" type="Host" minOccurs="1"
 maxOccurs="1">
 </xs:element>
 <xs:element name="ApplicationSystemType"
 type="ApplicationSystemType" minOccurs="1" maxOccurs="1">
 </xs:element>

 <xs:element name="SecureStoreData" type="SecureStoreData" minOccurs="0"
maxOccurs="1"/>

 <xs:element name="AccessPoints" minOccurs="0"
 maxOccurs="unbounded">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="AccessPoint"
 type="AccessPoint" minOccurs="1" maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>

 <xs:element name="Ports" minOccurs="0"
 maxOccurs="unbounded">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="Port" type="Port"
 minOccurs="1" maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>

 <xs:element name="SNMPAttributes" type="SNMPAttributes" minOccurs="0"
 maxOccurs="1">
 </xs:element>

 <xs:element name="Attributes" minOccurs="0"
 maxOccurs="unbounded">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="Attribute" type="Attribute"
 minOccurs="1" maxOccurs="unbounded" />
 </xs:sequence>
 </xs:complexType>
 </xs:element>

```

```

</xs:sequence>

<xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

<xs:attribute name="description" type="xs:string">
</xs:attribute>

<xs:attribute name="displaykey" type="xs:string"></xs:attribute>

<xs:attribute name="isTrusted" type="xs:boolean"></xs:attribute>

</xs:complexType>
<xs:complexType name="SNMPAttributes">
 <xs:annotation>
 <xs:documentation></xs:documentation>
 </xs:annotation>
 <xs:attribute name="snmpVersion" type="snmpVersionType" use="required">
</xs:attribute>

 <xs:attribute name="readCommunity" type="xs:string">
</xs:attribute>

 <xs:attribute name="writeCommunity" type="xs:string">
</xs:attribute>

 <xs:attribute name="userName" type="xs:string">
</xs:attribute>

 <xs:attribute name="authenticationProtocol" type="authenticationProtocolType">
</xs:attribute>

 <xs:attribute name="authenticationPassword" type="xs:string">
</xs:attribute>

 <xs:attribute name="privacyProtocol" type="privacyProtocolType">
</xs:attribute>

 <xs:attribute name="privacyPassword" type="xs:string">
</xs:attribute>

 <xs:attribute name="snmpRetries" type="xs:int" use="required">
</xs:attribute>

 <xs:attribute name="snmpTimeout" type="xs:long" use="required">
</xs:attribute>

 <xs:attribute name="deviceTypeName" type="xs:string"> </xs:attribute>

 <xs:attribute name="sysOid" type="xs:string">
</xs:attribute>
</xs:complexType>

<xs:complexType name="Host">
 <xs:annotation>
 <xs:documentation></xs:documentation>
 </xs:annotation>

 <xs:attribute name="ipaddress" type="xs:string"
 use="required">
</xs:attribute>

 <xs:attribute name="description" type="xs:string">
</xs:attribute>

```



```

 <xs:attribute name="ostype" type="xs:string"></xs:attribute>
</xs:complexType>

<xs:complexType name="ApplicationSystemType">
 <xs:annotation>
 <xs:documentation></xs:documentation>
 </xs:annotation>

 <xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

 <xs:attribute name="version" type="xs:string" use="required">
</xs:attribute>

</xs:complexType>

<xs:complexType name="AccessPoint">
 <xs:annotation>
 <xs:documentation></xs:documentation>
 </xs:annotation>

 <xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

 <xs:attribute name="description" type="xs:string">
</xs:attribute>

 <xs:attribute name="displaykey" type="xs:string"></xs:attribute>

 <xs:attribute name="type" type="AccessPointType"
 use="required">
</xs:attribute>

 <xs:attribute name="uri" type="xs:string"></xs:attribute>

 <xs:attribute name="host" type="xs:string" use="required">
</xs:attribute>

 <xs:attribute name="port" type="xs:string"></xs:attribute>

 <xs:attribute name="protocol" type="xs:string"></xs:attribute>

 <xs:attribute name="loginid" type="xs:string"></xs:attribute>

 <xs:attribute name="password" type="xs:string"></xs:attribute>

 <xs:attribute name="containerType" type="ContainerType"></xs:attribute>

 <xs:attribute name="order" type="xs:int" use="required">
</xs:attribute>

</xs:complexType>

<xs:complexType name="Port">
 <xs:annotation>
 <xs:documentation></xs:documentation>
 </xs:annotation>

 <xs:attribute name="name" type="xs:string" use="required">
</xs:attribute>

 <xs:attribute name="description" type="xs:string">
</xs:attribute>

 <xs:attribute name="protocol" type="xs:string" use="required"></xs:attribute>

```

```

 <xs:attribute name="port" type="xs:int" use="required"></xs:attribute>
 </xs:complexType>

 <xs:complexType name="Source">
 <xs:sequence>
 <xs:element name="Assignment" minOccurs="1"
 maxOccurs="unbounded">
 <xs:complexType>
 <xs:attribute name="name" type="xs:string">
 </xs:attribute>

 <xs:attribute name="targetAppSystemName"
 type="xs:string" use="required">
 </xs:attribute>

 <xs:attribute name="targetAppSystemTypeName"
 type="xs:string" use="required">
 </xs:attribute>

 <xs:attribute name="targetAppSystemTypeVersion"
 type="xs:string" use="required">
 </xs:attribute>

 <xs:attribute name="targetAppSystemHost"
 type="xs:string" use="required">
 </xs:attribute>

 <xs:attribute name="priority" type="xs:int"></xs:attribute>
 </xs:complexType>
 </xs:element>
 </xs:sequence>

 <xs:attribute name="sourceApplicationSystemName"
 type="xs:string" use="required">
 </xs:attribute>

 <xs:attribute name="sourceAppSystemTypeName" type="xs:string"
 use="required">
 </xs:attribute>

 <xs:attribute name="sourceAppSystemTypeVersion" type="xs:string"
 use="required">
 </xs:attribute>

 <xs:attribute name="sourceAppSystemHost" type="xs:string"
 use="required">
 </xs:attribute>
 </xs:complexType>

 <xs:complexType name="Attribute">
 <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
 <xs:attribute name="value" type="xs:string" use="required"></xs:attribute>
 <!-- added for secure store integration. -->
 <xs:attribute name="isencrypted" type="xs:boolean" use="optional"
 default="false"></xs:attribute>
 </xs:complexType>

 <xs:complexType name="SecureStoreData">
 <xs:attribute name="name" type="xs:string" use="required"></xs:attribute>
 <xs:attribute name="value" type="xs:string" use="required"></
xs:attribute>
 </xs:complexType>

 <xs:simpleType name="AccessPointType">

```

```

 <xs:restriction base="xs:string">
 <xs:enumeration value="TrustManagement" />
 <xs:enumeration value="EMURL" />
 <xs:enumeration value="WS" />
 <xs:enumeration value="GUI" />
 <xs:enumeration value="Other" />
 </xs:restriction>
 </xs:simpleType>

 <xs:simpleType name="ContainerType">
 <xs:restriction base="xs:string">
 <xs:enumeration value="JBOSS" />
 <xs:enumeration value="SIPAS" />
 </xs:restriction>
 </xs:simpleType>

 <xs:simpleType name="authenticationProtocolType">
 <xs:restriction base="xs:string">
 <xs:enumeration value="MD5" />
 <xs:enumeration value="SHA" />
 </xs:restriction>
 </xs:simpleType>

 <xs:simpleType name="privacyProtocolType">
 <xs:restriction base="xs:string">
 <xs:enumeration value="DES"/>
 <xs:enumeration value="3DES"/>
 <xs:enumeration value="AES128"/>
 <xs:enumeration value="AES192"/>
 <xs:enumeration value="AES256"/>
 </xs:restriction>
 </xs:simpleType>

 <xs:simpleType name="snmpVersionType">
 <xs:restriction base="xs:int">
 <xs:enumeration value="1"/>
 <xs:enumeration value="3"/>
 </xs:restriction>
 </xs:simpleType>
</xs:schema>

```

## Sample XML for bulk import of elements

```

<?xml version="1.0" encoding="UTF-8"?>
<RTSElements xsi:schemaLocation="http://www.avaya.com/rts ApplicationSystems.xsd "
xmlns="http://www.avaya.com/rts" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <ApplicationSystems>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test1">
 <Host description="Host" ipaddress="localhost" ostype="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test2">
 <Host description="Host" ipaddress="localhost" ostype="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test3">
 <Host description="Host" ipaddress="localhost" ostype="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test4">
 <Host description="Host" ipaddress="localhost" ostype="Host"/>
 </ApplicationSystem>
 </ApplicationSystems>
</RTSElements>

```

```

 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test5">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test6">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test7">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test8">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test9">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test10">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test11">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test12">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test13">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 <ApplicationSystem description="Test" displaykey="NewGateway1"
isTrusted="false" name="Test14">
 <Host description="Host" ipaddress="localhost" ostyle="Host"/>
 <ApplicationSystemType name="Other Applications" version="0"/>
 </ApplicationSystem>
 </ApplicationSystems>
 </RTSElements>

```

## XML Schema Definition for bulk import of Session Manager profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:smgr="http://xml.avaya.com/schema/import"
 targetNamespace="http://xml.avaya.com/schema/import_sessionmanager"
 elementFormDefault="qualified">

 <!--
 This is the XML schema for the "Session Manager Profile". It defines this

```

```

 profile inside of an XML document that defines a user record
 (see userimport.xsd)
-->

<xsd:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd"/>

<xsd:complexType name="SessionManagerCommProfXML">
 <xsd:complexContent>
 <xsd:extension base="smgr:xmlCommProfileType" />
 <xsd:sequence>
 <!--
 The following attributes are the names of objects that must
 already be administered in System Manager before performing
 the user import.

 The relative order here cannot be changed because it would
 break backwards compatibility with existing XML documents
 that could be used for an import.
 -->

 <!-- Name of the primary Session Manager (required) -->
 <xsd:element name="primarySM" type="xsd:string" minOccurs="1" />

 <!-- Name of the secondary Session Manager (optional) -->
 <xsd:element name="secondarySM" type="xsd:string" minOccurs="0" />

 <!-- Name of the Termination Application Sequence (optional) - administered
 under Session Manager /Application Configuration /Application Sequences
 -->
 <xsd:element name="terminationAppSequence" type="xsd:string" minOccurs="0" />

 <!-- Name of the Origination Application Sequence (optional)
 - administered under
 Session Manager /Application Configuration /Application Sequences --
 -->
 <xsd:element name="originationAppSequence" type="xsd:string" minOccurs="0" />

 <!-- Name of the Conference Factory Set (optional)
 - administered under
 Session Manager / Application Configuration / Conference Factories --
 -->
 <xsd:element name="confFactorySet" type="xsd:string" minOccurs="0" />

 <!-- Name of the Survivability Server (optional)
 - usually the name of a Branch Session Manager, but can be any non-CM
 SIP Entity -->
 <xsd:element name="survivabilityServer" type="xsd:string" minOccurs="0" />

 <!-- Name of the Home Location (required)
 - administered under Routing / Locations -->
 <xsd:element name="homeLocation" type="xsd:string" minOccurs="1" />

 <!-- The maximum number of endpoints that can be simultaneously
 registered using this Session Manager Profile. (optional)
 - The value is an integer between 1 and 10 and
 defaults to 1 if not specified. -->
 <xsd:element name="maxSimultaneousDevices" minOccurs="0">
 <xsd:simpleType>
 <xsd:restriction base="xsd:integer">
 <xsd:minInclusive value="1" />
 <xsd:maxInclusive value="10" />
 </xsd:restriction>
 </xsd:simpleType>
 </xsd:element>
 </xsd:sequence>
</complexType>

```

```

 </xsd:element>

 <!--
 If true, new registrations will be blocked for this Session Manager
 Profile if the maximum number of simultaneously registered endpoints
 (see "maxSimultaneousDevices" above) is currently registered. If
 false, an existing registration will be terminated to allow a new
 registration for this Session Manager Profile. (optional)
 - the value defaults to false if not specified
 -->
 <xsd:element name="blockNewRegistrationWhenMaxActive" minOccurs="0">
 <xsd:simpleType>
 <xsd:restriction base="xsd:boolean" />
 </xsd:simpleType>
 </xsd:element>

 </xsd:sequence>

 </xsd:extension>
</xsd:complexContent>
</xsd:complexType>

</xsd:schema>

```

### Sample XML for bulk import of Session Manager profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">

 <!-- User Record for: 5555555@domain.com -->
 <tns:user>

 (Other user elements are required here - consult the main user record
 XML schema reference)

 <!--
 This is the password for any SIP endpoints (phones) associated with the
 user's Session Manager Profile
 -->
 <commPassword>123456</commPassword>
 <!--
 (Other user elements may be required here - consult the main user record
 XML schema reference)
 -->
 <!-- Here, a Communication Profile is defined for the user -->
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>

 <!-- The user must be given one or more handles of type "SIP" to associate SIP
 devices with the Session Manager Profile. In this case, a SIP phone will
 be registered with a Session Manager as 5555555@domain.com -->
 <handleList>
 <handle>
 <handleName>5555555</handleName>
 <handleType>sip</handleType>
 <handleSubType>username</handleSubType>
 <domainName>domain.com</domainName>
 </handle>
 </handleList>

 <!-- Here, one or more product-specific profiles may be defined -->

```

```

 <!-- A Session Manager Profile is defined to associate a maximum of two
 SIP phones, having the SIP handle, 5555555@domain.com, with...
 "Primary Session Manager" ('Primary SM')
 "Secondary Session Manager" instance ('Secondary SM')
 "Termination Sequence" ('Sequence to My CM'),
 "Origination Sequence" ('Sequence to My CM'),
 "Conference Factory Set" ('EngineeringDepartmentConferenceSet')
 "Survivability Server" ("BSM" value below),
 "Home Location" ('My Home').
 If both phones are registered and a third phone tries to register
 using the same SIP handle, one of the two phones will have its
 registration terminated to allow the third phone to register.
 -->
<commProfileList>
 <commProfile xsi:type="ns3:SessionManagerCommProfXML"
xmlns:ns3="http://xml.avaya.com/schema/import_sessionmanager">
 <commProfileType>SessionManager</commProfileType>
 <ns3:primarySM>Primary SM</ns3:primarySM>
 <ns3:secondarySM>Secondary SM</ns3:secondarySM>
 <ns3:terminationAppSequence>Sequence to My CM</
ns3:terminationAppSequence>
 <ns3:originationAppSequence>Sequence to My CM</
ns3:originationAppSequence>
 <ns3:confFactorySet>EngineeringDepartmentConferenceSet</
ns3:confFactorySet>
 <ns3:survivabilityServer>BSM</ns3:survivabilityServer>
 <ns3:homeLocation>My Home</ns3:homeLocation>
 <ns3:maxSimultaneousDevices>3</ns3:maxSimultaneousDevices>
 <ns3:blockNewRegistrationWhenMaxActive>false</
ns3:blockNewRegistrationWhenMaxActive>
 </commProfile>

 <!--
 A CM Station Profile is associated with this Communication Profile.
 The application sequence, "Sequence to My CM", invoked by Session
 Manager for calls to and from 5555555@domain.com, sequences calls to
 the CM, "My CM".
 SIP devices associated with this Communication Profile are associated
 with the CM Station that has number 555-5555. The CM Station, 555-5555,
 already exists on the CM, so the "useExistingExtension" element has
 value "true".
 -->

 <commProfile xsi:type="ipt:xmlStationProfile" xmlns:ipt="http://
xml.avaya.com/schema/import_csm_cm">
 <commProfileType>CM</commProfileType>
 <ipt:cmName>My CM</ipt:cmName>
 <ipt:useExistingExtension>true</ipt:useExistingExtension>
 <ipt:extension>5555555</ipt:extension>
 </commProfile>

</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk import of endpoint profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://xml.avaya.com/
schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_cm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_cm">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

```

```

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlStationProfile">
 <xs:complexContent>
 <xs:extension base="one:xmlCommProfileType" >
 <xs:sequence>

 <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
 <xs:element name="cmName" type="xs:string" maxOccurs="1" minOccurs="1"/>
 <xs:element name="prefHandleId" type="xs:string" maxOccurs="1"
minOccurs="0"/>
 <!-- 'true' if already created extension is to be used. 'false' if
available extension is to be used. -->
 <xs:element name="useExistingExtension" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

 <!-- Extension Range which will be used to create Station using
available extension within given range -->
 <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Station extension number that need to be assigned to the user. -->
 <xs:element name="extension" maxOccurs="1" minOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|[nN][eE][xX]
[tT]"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Template name to be used to create station. Values defined in
Template will be used if not provided. -->
 <xs:element name="template" type="xs:string" maxOccurs="1"
minOccurs="0"/>

 <!-- Specifies the set type of the station -->
 <xs:element name="setType" type="xs:string" maxOccurs="1"
minOccurs="0"/>

 <!-- Security code for station. Value can be digit only. -->
 <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]*/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Valid values for port -->
 <!--01 to 64 First and second numbers are the cabinet number -->
 <!--A to E Third character is the carrier -->
 <!--01 to 20 Fourth and fifth characters are the slot number -->
 <!--01 to 32 Sixth and seventh characters are the circuit number -->
 <!--x or X Indicates that there is no hardware associated with the
port assignment since the switch was set up, and the administrator expects that the
extension would have a non-IP set. Or, the extension had a non-IP set, and it

```



```

dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony
(CTI) stations, as well as for SBS Extensions. -->
 <!--IP Indicates that there is no hardware associated with the port
assignment since the switch was set up, and the administrator expects that the
extension would have an IP set. This is automatically entered for certain IP station
set types, but you can enter for a DCP set with softphone permissions. This changes to
the s00000 type when the set registers. -->
 <xs:element name="port" type="xs:string" maxOccurs="1" minOccurs="0" />

 <!-- Whether the station should be deleted if it unassigned from the
user. -->
 <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

 <!-- Whether the endpoint name on CM should be overridden with the
value in User. -->
 <xs:element name="overRideEndpointName" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

 <!-- true/false for Enhanced Callr-Info display for 1-line phones -->
 <xs:element name="enhCallrInfodisplay" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

 <!-- true/false to enable/disable lock messages feature. -->
 <xs:element name="lockMessages" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
 <!-- Valid values: CM 5.2 - Path Number between 1-2000, time of day
table, t1-t999, or blank. -->
 <!-- Valid values: CM 6.0 - Path Number between 1-9999, time of day
table, t1-t999, or blank. -->
 <xs:element name="coveragePath1" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([1-9]{0})|(t[1-9][0-9]{0,2})|([1-9][0-9]
{0,3})"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- A coverage path is a prioritized sequence of extensions to which
your voice system will route an unanswered call. -->
 <!-- Valid values: CM 5.2 - Path Number between 1-2000, time of day
table, t1-t999, or blank. -->
 <!-- Valid values: CM 6.0 - Path Number between 1-9999, time of day
table, t1-t999, or blank. -->
 <xs:element name="coveragePath2" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([1-9]{0})|(t[1-9][0-9]{0,2})|([1-9][0-9]
{0,3})"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- The extension the system should hunt to for this telephone when
the telephone is busy. A station hunting chain can be created by assigning a hunt-to
station to a series of telephones. -->
 <xs:element name="huntToStation" type="xs:string" maxOccurs="1"
minOccurs="0" />

 <!-- Provides for partitioning of attendant groups and/or stations and
trunk groups. -->

```

```

 <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
 <!-- Valid values: 1 to 250 when TN is ON in special application and 1
to 100 o.w. -->
 <xs:element name="tn" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="250" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
 <!-- Typically this is used for multiple tenants in a building or
multiple departments within a company or organization. -->
 <!-- Valid values: 0 to 995 -->
 <xs:element name="cor" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0"/>
 <xs:maxInclusive value="995"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Class of Service lets you define groups of users and control those
groups' access to features -->
 <!-- Valid values: 1 to 15 -->
 <xs:element name="cos" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0" />
 <xs:maxInclusive value="15" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="xmobileType" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="EC500"/>
 <xs:enumeration value="DECT"/>
 <xs:enumeration value="IPDECT"/>
 <xs:enumeration value="PHS"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="mappingMode" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="termination"/>
 <xs:enumeration value="origination"/>
 <xs:enumeration value="both"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="configurationSet" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|[1-9][0-9][1-9]" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

```

```

 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="mobilityTrunkGroup" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9])
{2}|[1]([0-9]){3}|2000"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="dialPrefix" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9]*){0,4}"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="cellPhoneNumber" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{0,15}"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="musicSource" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="250" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="tests" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="dataModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <!-- Controls the behavior of speakerphones. -->
 <xs:element name="speakerphone" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="none"/>
 <xs:enumeration value="1-way"/>
 <xs:enumeration value="2-way"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- The language that displays on stations -->
 <!-- Time of day is displayed in 24-hour format (00:00 - 23:59) for all
languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59
p.m.). -->
 <!-- unicode: Displays English messages in a 24-hour format . If no
Unicode file is installed, displays messages in English by default. -->
 <xs:element name="displayLanguage" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="english"/>

```

```

 <xs:enumeration value="french"/>
 <xs:enumeration value="italian"/>
 <xs:enumeration value="spanish"/>
 <xs:enumeration value="unicode"/>
 <xs:enumeration value="unicode2"/>
 <xs:enumeration value="unicode3"/>
 <xs:enumeration value="unicode4"/>
 <xs:enumeration value="user-defined"/>
 </xs:restriction>
</xs:simpleType>
</xs:element>

<!-- Defines the personalized ringing pattern for the station.
 Personalized Ringing allows users of some telephones to have one of
 8 ringing patterns for incoming calls.
 For virtual stations, this field dictates the ringing pattern on
 its mapped-to physical telephone.
-->
<!-- L = 530 Hz, M = 750 Hz, and H = 1060 Hz -->
<!-- Valid Entries Usage
 1 MMM (standard ringing)
 2 HHH
 3 LLL
 4 LHH
 5 HHL
 6 HLL
 7 HLH
 8 LHL
-->
<xs:element name="personalizedRingingPattern" maxOccurs="1"
minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="8" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- The Message Lamp Extension associated with the current extension --
>
<xs:element name="messageLampExt" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]+([\.\-][0-9]+)*"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- Enables or disables the mute button on the station. -->
<xs:element name="muteButtonEnabled" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!--
 When used with Multi-media Call Handling, indicates which extension
 is assigned to the data module of the multimedia complex. Users can
 dial this extension to place either a voice or a data call, and voice
 conversion, coverage, and forwarding apply as if the call were made
 to the 1-number.
-->
<!--

```

Valid Entry Usage A valid BRI data extension For MMCH, enter the extension of the data module that is part of this multimedia complex.

H.323 station extension For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application. blank Leave this field blank for single-connect IP applications.

```
-->
<xs:element name="mediaComplexExt" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([1-9]{0})|([0-9]+([\.\-][0-9]+)*)" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- Whether this is IP soft phone. -->
<xs:element name="ipSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!--
Survivable GK Node Name Identifies the existence of other H.323
gatekeepers located within gateway products that offer survivable
call
features. For example, the MultiTech MVPxxx-AV H.323 gateway family
and the SLS function within the H.248 gateways. When a valid IP node
name is entered into this field, Communication Manager adds the IP
address of this gateway to the bottom of the Alternate Gatekeeper
List
for this IP network region. As H.323 IP stations register with
Communication Manager, this list is sent down in the registration
confirm message. This allows the IP station to use the IP address of
this Survivable Gatekeeper as the call controller of last resort to
register with. Available only if the station type is an H.323
station
(46xxor 96xx models).
Valid Entry Usage
Valid IP node name Any valid previously-administered IP
node name.
blank There are no external gatekeeper nodes
within a customer's network. This is the default value.
-->
<xs:element name="survivableGkNodeName" type="xs:string" maxOccurs="1"
minOccurs="0" />

<!--
Sets a level of restriction for stations to be used with the
survivable dial plan to limit certain users to only to certain types
of calls. You can list the restriction levels in order from the most
restrictive to least restrictive. Each level assumes the calling
ability of the ones above it. This field is used by PIM module of
the
Integrated Management to communicate with the Communication Manager
administration tables and obtain the class of service information.
PIM
module builds a managed database to send for Standard Local
Survivability (SLS) on the H.248 gateways. Available for all analog
and IP station types.

Valid Entries Usage
emergency This station can only be used to place
```

emergency calls.

|          |                                                |
|----------|------------------------------------------------|
| internal | This station can only make intra-switch calls. |
|----------|------------------------------------------------|

This is the default.

|       |                                                                                                                                         |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------|
| local | This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables. |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------|

|      |                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|
| toll | This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables. |
|------|---------------------------------------------------------------------------------------------------------------------------------------------|

|              |                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| unrestricted | This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users. |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```
-->
<xs:element name="survivableCOR" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="emergency"/>
 <xs:enumeration value="internal"/>
 <xs:enumeration value="local"/>
 <xs:enumeration value="toll"/>
 <xs:enumeration value="unrestricted"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Designates certain telephones as not being allowed to receive
incoming
 trunk calls when the Media Gateway is in survivable mode. This field
successfully
 is used by the PIM module of the Integrated Management to
obtain
 interrogate the Communication Manager administration tables and
database
 the class of service information. PIM module builds a managed
IP
 to send for SLS on the H.248 gateways. Available for all analog and
 station types.

 Valid Entry Usage
 true Allows this station to be an incoming trunk
destination while the Media Gateway is running in survivability mode. This is the
default.
 false Prevents this station from receiving incoming
trunk calls when in survivable mode.

-->
<xs:element name="survivableTrunkDest" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- Enter the complete Voice Mail Dial Up number. -->
<xs:element name="voiceMailNumber" maxOccurs="1" minOccurs="0" >

 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[(0-9)(*)(#)(~mwWps)]{0,24}"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- Analog telephones only. -->
<!--
Valid entries Usage
true Enter true if this telephone is not located in the
same building with the system. If you enter true, you must complete R Balance Network.
```

```

false Enter false if the telephone is located in the
same building with the system.
-->
<xs:element name="offPremisesStation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- If a second line on the telephone is administered on the I-2
channel, enter analog. Otherwise, enter data module if applicable or none. -->
<xs:element name="dataOption" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="analog"/>
 <xs:enumeration value="data-module"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<xs:element name="displayModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- if led or neon then messageLampExt should be enable otherwise its
blank -->
<xs:element name="messageWaitingIndicator" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="led"/>
 <xs:enumeration value="neon"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- Enter true to use this station as an endpoint in a remote office
configuration. -->
<xs:element name="remoteOfficePhone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- Defines the source for Leave Word Calling (LWC) messages. -->
<!--
Valid entries Usage
audix If LWC is attempted, the messages are stored
in AUDIX.
spe If LWC is attempted, the messages are stored in
the system processing element (spe).
none If LWC is attempted, the messages are not
stored.

-->
<xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="audix"/>
 <xs:enumeration value="msa"/>
 <xs:enumeration value="spe"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
Enter true to allow internal telephone users to leave short LWC
messages
for this extension. If the system has hospitality, enter true for

```

```

 guest-room telephones if the extension designated to receive failed
 wakeup messages should receive LWC messages that indicate the wakeup
 calls failed. Enter true if LWC Reception is audix.
-->
<xs:element name="lwcActivation" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="lwcLogExternalCalls" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="cdrPrivacy" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="redirectNotification" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="perButtonRingControl" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="bridgedCallAlerting" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="bridgedIdleLinePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
<xs:element name="confTransOnPrimaryAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
<xs:element name="customizableLabels" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="expansionModule" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="ipVideoSoftphone" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<xs:element name="activeStationRinging" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="single"/>
 <xs:enumeration value="continuous"/>
 <xs:enumeration value="if-busy-single"/>
 <xs:enumeration value="silent"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- Defines how call rings to the telephone when it is on-hook.-->
<!--
Valid entries Usage
continuous Enter continuous to cause all calls to
this telephone to ring continuously.
if-busy-single Enter if-busy-single to cause calls to
this telephone to ring continuously when the telephone is off-hook and idle and calls
to this telephone to
 receive one ring cycle and then ring
silently when the telephone is off-hook and active.
silent-if-busy Enter silent-if-busy to cause calls to
ring silently when this station is busy.
single Enter single to cause calls to this
telephone to receive one ring cycle and then ring silently.
-->
<xs:element name="idleActiveRinging" type="xs:string" maxOccurs="1"
minOccurs="0" /> <!-- not found in xhtml -->

<!-- Must be set to true when the Type field is set to H.323. -->
<xs:element name="switchhookFlash" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- If this field is true, the short switch-hook flash (50 to 150)
from a 2500-type set is ignored. -->
<xs:element name="ignoreRotaryDigits" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

```



```

 <!--
 H.320 Conversion - Valid entries are true and false (default). This
field is
 optional for non-multimedia complex voice stations and for Basic
 multimedia complex voice stations. It is mandatory for Enhanced
 multimedia complex voice stations. Because the system can only
handle
 a limited number of conversion calls, you might need to limit the
 number of telephones with H.320 conversion. Enhanced multimedia
 complexes must have this flag set to true.
 -->
 <xs:element name="h320Conversion" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!--
 The service link is the combined hardware and software multimedia
 connection between an Enhanced mode complex's H.320 DVC system and
the
 Avaya DEFINITY Server which terminates the H.320 protocol. A service
 link is never used by a Basic mode complex H.320 DVC system.
 Connecting a service link will take several seconds. When the
service
 link is connected, it uses MMI, VC and system timeslot resources.
When
 the service link is disconnected it does not tie up any resources.
 The
 Service Link Mode can be administered as either 'as-needed' or
 'permanent' as described below: - As-Needed - Most non-call center
 multimedia users will be administered with this service link mode.
The
 as-needed mode provides the Enhanced multimedia complex with a
 connected service link whenever a multimedia call is answered by the
 station and for a period of 10 seconds after the last multimedia
call
 on the station has been disconnected. Having the service link stay
 connected for 10 seconds allows a user to disconnect a multimedia
call
 and then make another multimedia call without having to wait for the
 service link to disconnect and re-establish. - Permanent -
Multimedia
 call center agents and other users who are constantly making or
 receiving multimedia calls might want to be administered with this
 service link mode. The permanent mode service link will be connected
 during the station's first multimedia call and will remain in a
 connected state until the user disconnects from their PC's
multimedia
 application or the Avaya DEFINITY Server restarts. This provides a
 multimedia user with a much quicker video cut-through when
answering a
 multimedia call from another permanent mode station or a multimedia
call that has been early answered. • Multimedia Mode - There are two
 multimedia modes, Basic and Enhanced, as
 -->
 <xs:element name="serviceLinkMode" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="as-needed"/>
 <xs:enumeration value="permanent"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--
 There are two multimedia modes, Basic and Enhanced, as described

```

below:

Basic - A Basic multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone set. When in Basic mode, users place voice calls at the multifunction telephone and multimedia calls from the multimedia equipped PC. Voice calls will be answered at the multifunction telephone and multimedia calls will alert first at the PC and if unanswered will next alert at the voice station if it is administered with H.320 enabled. A Basic mode complex has limited multimedia feature capability.

Enhanced - An Enhanced multimedia complex consists of a BRI-connected multimedia-equipped PC and a non-BRI-connected multifunction telephone. The Enhanced mode station acts as though the PC were directly connected to the multifunction telephone; the link provides the actual connection between the Avaya DEFINITY and the PC. Thus, voice and multimedia calls are originated and received at the telephone set. Voice and multimedia call status are also displayed at the telephone set. An Enhanced mode station allows multimedia calls to take full advantage of most call control features

```
-->
<xs:element name="multimediaMode" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="basic"/>
 <xs:enumeration value="enhanced"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- Controls the auditing or interrogation of a served user's message
waiting indicator (MWI).
Valid entries Usage
fp-mwi Use if the station is a served user of an fp-
mwi message center.
qsig-mwi Use if the station is a served user of a qsig-
mwi message center.
blank Leave blank if you do not want to audit the
served user's MWI or if the user is not a served user of either an
fp-mwi or qsig-mwi message center.
-->
<xs:element name="mwiServedUserType" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="fp-mwi"/>
 <xs:enumeration value="qsig-mwi"/>
 <xs:enumeration value="sip-adjunct"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!-- The AUDIX associated with the station.
Must contain a user-defined adjunct name that was previously
administered.
-->
 <xs:element name="audixName" type="xs:string" maxOccurs="1"
minOccurs="0" />

<!--
Automatic Moves allows a DCP telephone to be unplugged from one
location and moved to a new location without additional
```

Communication Manager administration. Communication Manager automatically associates the extension to the new port.

\*\*\*\*\*CAUTION\*\*\*\*\*  
When a DCP telephone is unplugged and moved to another physical location, the Emergency Location Extension field must be changed for that extension or the USA Automatic Location Identification data base must be manually updated. If the Emergency Location Extension field is not changed or if the USA Automatic Location Identification data base is not updated, the DID number sent to the Public Safety Network could send emergency response personnel to the wrong location.

Valid entries                      Usage  
always                              Enter always and the DCP telephone can be moved anytime without additional administration by unplugging from one location and plugging into a new location.  
once                                Enter once and the DCP telephone can be unplugged and plugged into a new location once. After a move, the field is set to done the next time that routine maintenance runs on the DCP telephone. Use once when moving a large number of DCP telephones so each extension is removed from the move list. Use once to prevent automatic maintenance replacement.  
no                                  Enter no to require administration in order to move the DCP telephone. Done is a display-only value. Communication Manager sets the field to done after the telephone is moved and routine maintenance runs on the DCP telephone.  
error                              Error is a display-only value. Communication Manager sets the field to error, after routine maintenance runs on the DCP telephone, when a non-serialized telephone is set as a movable telephone.

```
-->
<xs:element name="automaticMoves" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="always"/>
 <xs:enumeration value="no"/>
 <xs:enumeration value="once"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Tells Communication Manager how to handle emergency calls from the
 IP telephone.

 *****CAUTION*****
 An Avaya IP endpoint can
 dial emergency calls (for example, 911 calls in the U.S.). It only
```

|                                 |                                                                      |                                             |
|---------------------------------|----------------------------------------------------------------------|---------------------------------------------|
| reaches                         | the local emergency service in the Public Safety Answering Point     |                                             |
| area                            | where the telephone system has local trunks. Please be advised that  |                                             |
| an                              | Avaya IP endpoint cannot dial to and connect with local emergency    |                                             |
|                                 | service when dialing from remote locations that do not have local    |                                             |
| for                             | trunks. Do not use an Avaya IP endpoint to dial emergency numbers    |                                             |
|                                 | emergency services when dialing from remote locations. Avaya Inc. is |                                             |
|                                 | not responsible or liable for any damages resulting from misplaced   |                                             |
| product                         | emergency calls made from an Avaya endpoint. Your use of this        |                                             |
|                                 | indicates that you have read this advisory and agree to use an       |                                             |
|                                 | alternative telephone to dial all emergency calls from remote        |                                             |
|                                 | locations. Please contact your Avaya representative if you have      |                                             |
| if                              | questions about emergency calls from IP telephones. Available only   |                                             |
|                                 | the station is an IP Softphone or a remote office station.           |                                             |
|                                 | Valid entries                                                        | Usage                                       |
|                                 | as-on-local                                                          | Type as-on-local to achieve the             |
| following results:              |                                                                      |                                             |
| Emergency Location              |                                                                      | If the administrator chooses to leave the   |
| station's IP address) on        |                                                                      | Extension fields (that correspond to this   |
| value as-on-local               |                                                                      | the IP Address Mapping screen blank, the    |
| Emergency Location              |                                                                      | sends the extension entered in the          |
| the Public Safety               |                                                                      | Extension field in the Station screen to    |
| Address Mapping screen with     |                                                                      | Answering Point (PSAP).                     |
| functions as follows:           |                                                                      | If the administrator populates the IP       |
| in the Station screen           |                                                                      | emergency numbers, the value as-on-local    |
| Extension field in the          |                                                                      | - If the Emergency Location Extension field |
| local sends the                 |                                                                      | is the same as the Emergency Location       |
| Point (PSAP).                   |                                                                      | IP Address Mapping screen, the value as-on- |
| in the Station screen           |                                                                      | extension to the Public Safety Answering    |
| Extension field in the          |                                                                      | - If the Emergency Location Extension field |
| local sends the                 |                                                                      | is different from the Emergency Location    |
| to the Public Safety            |                                                                      | IP Address Mapping screen, the value as-on- |
|                                 |                                                                      | extension in the IP Address Mapping screen  |
|                                 |                                                                      | Answering Point (PSAP).                     |
|                                 | block                                                                | Enter block to prevent the completion of    |
| emergency calls. Use this entry |                                                                      | for users who move around but always have a |
| circuit-switched telephone      |                                                                      | nearby, and for users who are farther away  |
| from the Avaya S8XXX Server     |                                                                      | than an adjacent area code served by the    |
| same 911 Tandem office.         |                                                                      | When users attempt to dial an emergency     |

call from an IP Telephone and  
a nearby circuit-switched

to send the CESID

the PSAP. The end user

IP Softphone.

warrior service that are near

emergency call routed over

the server or switch.

emergency calls, the digit string is the

is a local direct-dial number

location of the IP Softphone. If the

calls, the end user enters a

location, based on advice from

the option (extension, block, or

registration and the IP Softphone

that can be swapped back and

with a fixed location.

the softphone. A DCP or

selects extension.

```
-->
<xs:element name="remoteSoftphoneEmergencyCalls" maxOccurs="1"
minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="as-on-local"/>
 <xs:enumeration value="block"/>
 <xs:enumeration value="cesid"/>
 <xs:enumeration value="option"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>
```

<!-- This field allows the system to properly identify the location of a caller who dials a 911 emergency call from this station. An entry in this field must be of an extension type included in the dial plan, but does not have to be an extension on the local system. It can be a UDP extension. The entry defaults to blank. A blank entry typically would be used for an IP softphone dialing in through PPP from somewhere

the call is blocked, they can dial 911 from telephone instead.

Enter cesid to allow Communication Manager information supplied by the IP Softphone to enters the emergency information into the Use this entry for IP Softphones with road enough to the Avaya S8XXX Server that an the it's trunk reaches the PSAP that covers If the server uses ISDN trunks for telephone number, provided that the number with the local area code, at the physical server uses CAMA trunks for emergency specific digit string for each IP Softphone the local emergency response personnel.

Enter option to allow the user to select cesid) that the user selected during reported. Use this entry for extensions forth between IP Softphones and a telephone The user chooses between block and cesid on IP telephone in the office automatically

outside your network. If you populate the IP Address Mapping screen with emergency numbers, the feature functions as follows: If the Emergency Location Extension field in the Station screen is the same as the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension to the Public Safety Answering Point (PSAP). If the Emergency Location Extension field in the Station screen is different from the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension in the IP Address Mapping screen to the Public Safety Answering Point (PSAP).

```
-->
<xs:element name="emergencyLocationExt" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]+([\.\-][0-9]+)*/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 A softphone can register no matter what emergency call handling
 settings the user has entered into the softphone. If a softphone dials 911,
 the administered Emergency Location Extension is used. The softphone's
 user-entered settings are ignored. If an IP telephone dials 911, the
 administered Emergency Location Extension is used. If a call center
 agent dials 911, the physical station extension is displayed,
 overriding the administered LoginID for ISDN Display . Does not
 apply to SCCAN wireless telephones, or to extensions administered as type
 h.323.
-->
<xs:element name="alwaysUse" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!-- Activates or deactivates Precedence Call Waiting for this station
-->
<xs:element name="precedenceCallWaiting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

<!--
 Enables or disables automatic selection of any idle appearance for
 attempts transferred or conferenced calls. Communication Manager first
 to find an idle appearance that has the same extension number as the
 call being transferred or conferenced has. If that attempt fails,
 Communication Manager selects the first idle appearance.
-->
<xs:element name="autoSelectAnyIdleAppearance"
type="xs:boolean" maxOccurs="1" minOccurs="0" />

<!--
 Allows or denies users in the telephone's Coverage Path to retrieve
 if Leave Word Calling (LWC) messages for this telephone. Applies only
 the telephone is enabled for LWC Reception.
-->
<xs:element name="coverageMsgRetrieval" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<!--
 In EAS environments, the auto answer setting for the Agent LoginID
```

can override a station's setting when an agent logs in.

|             |                                                                                                                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Valid Entry | Usage                                                                                                                                                                                                                                                                              |
| all         | All ACD and non-ACD calls terminated to an idle station cut through immediately.                                                                                                                                                                                                   |
|             | Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the Allow Ringer-off with Auto-Answer is enabled for the system. |
| acd         | Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls terminated to a station ring audibly.                                                                                                                                                             |
|             | For analog stations, the station is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.          |
| none        | All calls terminated to this station receive an audible ringing treatment.                                                                                                                                                                                                         |
| icom        | Allows a telephone user to answer an intercom call from the same intercom group without pressing the intercom button.                                                                                                                                                              |

```

-->
<xs:element name="autoAnswer" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="acd"/>
 <xs:enumeration value="all"/>
 <xs:enumeration value="icom"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Enables or disables data restriction that is used to prevent tones,
 such as call-waiting tones, from interrupting data calls.
 Data restriction provides permanent protection and cannot be
 changed by the telephone user. Cannot be assigned if Auto Answer
 is administered as all or acd. If enabled, whisper page to this
 station is denied.
-->
<xs:element name="dataRestriction" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

<!--
 Indicates which call appearance is selected when the user lifts the
 handset and there is an incoming call.
 Valid Entry Usage
 true The user connects to an idle call
 appearance instead of the ringing call.
 false The Alerting Appearance Preference is
 set and the user connects to the ringing call appearance.
-->
<xs:element name="idleAppearancePreference" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

<!--
 enable/disable call waiting for this station
-->
<xs:element name="callWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

```

```

 <!--
 Attendant call waiting allows attendant-originated or attendant-
 extended calls to a busy
 single-line telephone to wait and sends distinctive call-waiting
 tone to the single-line user.
 Enable/disable attendant call waiting
 -->
 <xs:element name="attCallWaitingIndication" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!--
 Enter true so the telephone can receive the 3 different types of
 ringing patterns which identify the type of incoming calls.
 Distinctive ringing might not work properly for off-premises
 telephones. -->
 <xs:element name="distinctiveAudibleAlert" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!--
 Valid Entries Usage
 true Restricts the last idle call appearance
 used for incoming priority calls and outgoing call originations only.
 false Last idle call appearance is used for
 incoming priority calls and outgoing call originations.
 -->
 <xs:element name="restrictLastAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!--
 Valid entries Usage
 true Analog disconnect signal is sent
 automatically to the port after a call terminates. Analog devices
 (such as answering machines and
 speakerphones) use this signal to turn the devices off after a call terminates.
 false Hunt group agents are alerted to incoming
 calls. In a hunt group environment, the disconnect
 signal blocks the reception of zip tone and
 incoming call notification by an auto-answer station when a call
 is queued for the station.
 -->
 <xs:element name="adjunctSupervision" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <!--
 Send Calling Number.
 Valid Entries Usage
 y All outgoing calls from the station will
 deliver the Calling Party Number
 (CPN) information as "Presentation Allowed."
 n No CPN information is sent for the call
 r Outgoing non-DCS network calls from the
 station will deliver the Calling
 Party Number information as "Presentation
 Restricted."
 -->
 <xs:element name="perStationCpnSendCallingNumber" maxOccurs="1"
minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="r"/>
 <xs:enumeration value="n"/>
 <xs:enumeration value="y"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

```



```

 <!--
 Appears on the Station screen for analog telephones, only if the
Without Flash field in the
 ANALOG BUSY AUTO CALLBACK section of the Feature-Related System
Parameters
 screen is set to true. The Busy Auto Callback without Flash field
then defaults to true for all analog
 telephones that allow Analog Automatic Callback.
 Set true to provide automatic callback for a calling analog station
without flashing the hook.
 -->
 <xs:element name="busyAutoCallbackWithoutFlash" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!-- Provides audible message waiting. -->
 <xs:element name="audibleMessageWaiting" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!-- Provides extended local calls / imsFeatureSequencing
 Extended Local Calls (ELC) /imsFeatureSequencing allows DCP and H.323
stations to use SIP sequenced applications. The feature works by routing calls
 involving those stations over SIP IMS trunks. In other words, CM is
applying the half-call model to those stations.
 That also has the side effect that features which work differently
under the half-call model than under the usual (full-call) model
 also work differently for ELC stations.
 The Extended Local Calls feature is administrable per station. We're
allowing stations that always use SIP IMS trunks to coexist on
 the same server with stations that dont always use SIP IMS trunks. In
other words, ELC is changing a previous marketing rule that
 the full-call model (CM-ES) and the half-call model (CM-FS) functions
can't co-exist on the same server. As noted above, that also
 has the side effect that features which work differently under the half-
call model than under the full-call model now also can work
 differently for two different SIP stations on the same CM
server.
 -->
 <xs:element name="imsFeatureSequencing" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <!--
 Only administrable if Hospitality is enabled on the System
Parameters
 Customer-Options (Optional Features) screen. This field affects the
telephone display on calls that originated from a station with
Client
 Room Class of Service. Note: For stations with an audix station
type, AUDIX Voice Power ports, or ports for any other type of
messaging that needs display information, Display Client Redirection
must be enabled.
 Set true to redirect information for a call originating from a
Client Room and terminating to this station displays.
 -->
 <xs:element name="displayClientRedirection" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!--
 Valid Entries Usage
 true Indicates that a station's line selection is
not to be moved from the currently selected line button
 to a different, non-alerting line button. If
you enter true, the line selection on an on-hook station only moves from the last
 used line button to a line button with an
audibly alerting call. If there are no alerting calls, the line selection

```

```

 remains on the button last used for a call.
 false The line selection on an on-hook station with
no alerting calls can be moved to a different line button, which might be serving a
different
 extension.

 -->
 <xs:element name="selectLastUsedAppearance" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!-- Whether an unanswered forwarded call is provided coverage
treatment. -->
 <xs:element name="coverageAfterForwarding" type="xs:string"
maxOccurs="1" minOccurs="0" />

 <!-- Allow/disallow direct audio connections between IP endpoints. -->
 <xs:element name="directIpIpAudioConnections" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <!-- Allows IP endpoints to be connected through the server's IP
circuit pack. -->
 <xs:element name="ipAudioHairpinning" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="primeAppearancePreference" type="xs:string"
maxOccurs="1" minOccurs="0" />

 <!-- Elements with complex data type. Please refer the appropriate
elements for more details. -->
 <xs:element name="stationSiteData" type="csm:xmlStationSiteData"
maxOccurs="1" minOccurs="0" />
 <xs:element name="abbrList" type="csm:xmlStationAbbreviatedDialingData"
maxOccurs="unbounded" minOccurs="0" />
 <xs:element name="buttons" type="csm:xmlButtonData" maxOccurs="24"
minOccurs="0" />
 <xs:element name="featureButtons" type="csm:xmlButtonData"
maxOccurs="24" minOccurs="0" />
 <xs:element name="expansionModuleButtons" type="csm:xmlButtonData"
maxOccurs="72" minOccurs="0" />
 <xs:element name="softKeys" type="csm:xmlButtonData" maxOccurs="15"
minOccurs="0" />
 <xs:element name="displayButtons" type="csm:xmlButtonData"
maxOccurs="unbounded" minOccurs="0" />
 <xs:element name="stationDataModule" type="csm:xmlStationDataModule"
maxOccurs="1" minOccurs="0" />
 <xs:element name="hotLineData" type="csm:xmlStationHotLineData"
maxOccurs="1" minOccurs="0" />
 <xs:element name="nativeName" type="csm:xmlNativeNameData"
maxOccurs="1" minOccurs="0"/>

 <!-- Number of button modules 0-3-->
 <xs:element name="buttonModules" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0" />
 <xs:maxInclusive value="3" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="unconditionalInternalDest" maxOccurs="1"
minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">

```

```

 <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}{#}|
[*][0-9]{1,17}|[0-9]{1,18}|[*]{#}|"/>
 </xs:restriction>
</xs:simpleType>
</xs:element>

 <xs:element name="unconditionalInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <xs:element name="unconditionalExternalDest" maxOccurs="1"
minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}{#}|
[*][0-9]{1,17}|[0-9]{1,18}|[*]{#}|"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="unconditionalExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <xs:element name="busyInternalDest" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}{#}|
[*][0-9]{1,17}|[0-9]{1,18}|[*]{#}|"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="busyInternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="busyExternalDest" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}{#}|
[*][0-9]{1,17}|[0-9]{1,18}|[*]{#}|"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="busyExternalActive" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="noReplyInternalDest" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}{#}|
[*][0-9]{1,17}|[0-9]{1,18}|[*]{#}|"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="noReplyInternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <xs:element name="noReplyExternalDest" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[*][0-9]{1,16}{#}|[0123456789]{1,17}{#}|
[*][0-9]{1,17}|[0-9]{1,18}|[*]{#}|"/>

```

```

 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="noReplyExternalActive" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <xs:element name="sacCfOverride" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="a"/>
 <xs:enumeration value="n"/>
 <xs:enumeration value="y"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="lossGroup" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="19" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="timeOfDayLockTable" maxOccurs="1"
minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[1-5][0-9]{0}" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="emuLoginAllowed" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="ec500State" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="enabled"/>
 <xs:enumeration value="disabled"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- true/false to enable/disable Mute on Off Hook in Shared Control
Mode feature. -->
 <xs:element name="muteOnOffHookInSCMode" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

 <xs:element name="type3pccEnabled" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="None"/>
 <xs:enumeration value="Avaya"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="sipTrunk" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="aar|ars|[1-9]|[1-9][0-9]|[1-9]([0-9]){2}|"

```

```

[1] ([0-9]){3}|2000"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

 <xs:element name="multimediaEarlyAnswer" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
 <xs:element name="bridgedApprOrigRestr" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="callApprDispFormat" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="inter-location"/>
 <xs:enumeration value="intra-location"/>
 <xs:enumeration value="disp-param-default"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Enter a Group ID between 0-999, or blank -->
 <xs:element name="ipPhoneGroupId" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]|[0-9][0-9]|[0-9][0-9][0-9]|[0-9]
{0}"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="xoipEndPointType" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="auto"/>
 <xs:enumeration value="fax"/>
 <xs:enumeration value="modem"/>
 <xs:enumeration value="tty"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="xid" type="xs:boolean" maxOccurs="1" minOccurs="0" />
 <xs:element name="stepClearing" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
 <xs:element name="fixedTei" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="tei" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-6][0-3]"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="countryProtocol" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="1"/>
 <xs:enumeration value="2"/>
 <xs:enumeration value="3"/>
 <xs:enumeration value="6"/>
 <xs:enumeration value="etsi"/>
 </xs:restriction>
 </xs:simpleType>

```

```

 </xs:element>

 <xs:element name="endptInit" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="spid" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{1,10}" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="endptId" maxOccurs="1" minOccurs="0" > <!-- 00 to 62
-->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-6][0-2]" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="isMCTSignalling" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
 <xs:element name="isShortCallingPartyDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
 <xs:element name="passageWay" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
 <xs:element name="dtmfOverIp" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="in-band" />
 <xs:enumeration value="in-band-g711" />
 <xs:enumeration value="out-of-band" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="location" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[1-9]{0} | [1-9] | [1-9][0-9] | [1-9]([0-9])
{2} | [1]([0-9]){3} | 2000" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlStationSiteData">
 <xs:sequence>
 <xs:element name="room" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="10" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="jack" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">

```

```

 <xs:maxLength value="5"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="cable" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="5"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="floor" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="building" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="headset" type="xs:boolean" maxOccurs="1" minOccurs="0" />
 <xs:element name="speaker" type="xs:boolean" maxOccurs="1" minOccurs="0" />

 <xs:element name="mounting" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="d"/>
 <xs:enumeration value="w"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Enter numeric cord length (0-99) -->
 <xs:element name="cordLength" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0" />
 <xs:maxInclusive value="99" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="setColor" type="xs:string" maxOccurs="1" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="xmlStationAbbreviatedDialingData">
 <xs:sequence>
 <xs:element name="listType" maxOccurs="1" minOccurs="1" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="enhanced"/>
 <xs:enumeration value="group"/>
 <xs:enumeration value="personal"/>
 <xs:enumeration value="system"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" />
 <xs:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlButtonData">
 <xs:sequence>
 <xs:element name="number" type="xs:int" maxOccurs="1" minOccurs="1" /><!--
*****Must present***** -->
 <xs:element name="type" type="xs:string" maxOccurs="1" minOccurs="1" /><!--
*****Must present***** -->

```

```

 <xs:element name="data1" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="data2" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="data3" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="data4" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="data5" type="xs:string" maxOccurs="1" minOccurs="0" />
 <xs:element name="data6" type="xs:string" maxOccurs="1" minOccurs="0" />
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationDataModule">
 <xs:sequence>
 <xs:element name="dataExtension" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]+([.-][0-9]+)*/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="name" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="29"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="cor" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0" />
 <xs:maxInclusive value="995" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="cos" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0" />
 <xs:maxInclusive value="15" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="itc" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="restricted"/>
 <xs:enumeration value="unrestricted"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <!-- CM dependant field - 100 or 250 depends on system params -->
 <xs:element name="tn" maxOccurs="1" minOccurs="1" ><!-- *****Must
present***** -->
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="250" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="listType" maxOccurs="1" minOccurs="0" >

```



```

 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="enhanced"/>
 <xs:enumeration value="group"/>
 <xs:enumeration value="personal"/>
 <xs:enumeration value="system"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="listId" type="xs:int" maxOccurs="1" minOccurs="0" />

 <xs:element name="specialDialingOption" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="default"/>
 <xs:enumeration value="hot-line"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="specialDialingAbbrDialCode" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="4"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlStationHotLineData">
 <xs:sequence>
 <xs:element name="hotLineDestAbbrevList" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="3" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="hotLineAbbrevDialCode" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]*"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 </xs:sequence>
</xs:complexType>

<!-- If displayName,givenName or surname contains characters of multiple scripts then
locale tag should be present.
If displayName tag is present then it overwrites native name.
If displayname is not present then combination of givenName and surname gets
copied in native name.
Please find below locale for multiscript language
Language Locale
Japanese ja, ja-jp
Simplified Chinese zh-cn
Traditional Chinese zh-tw -->
<xs:complexType name="xmlNativeNameData">
 <xs:sequence>
 <xs:element name="locale" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="ja-jp"/>

```

```

 <xs:enumeration value="ja"/>
 <xs:enumeration value="zh-cn"/>
 <xs:enumeration value="zh-tw"/>
 >
 </xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="name" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="27"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

### Sample XML for bulk import of endpoint profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>BASIC</authenticationType>
 <description>description</description>
 <displayName>displayname</displayName>
 <displayNameAscii>displayNameAscii</displayNameAscii>
 <dn>dn</dn>
 <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>givenName00</givenName>
 <honorific>honorific</honorific>
 <loginName>user00_00xyz@avaya.com</loginName>
 <middleName>middleName</middleName>
 <managerName>managerName</managerName>
 <preferredGivenName>preferredGivenName</preferredGivenName>
 <preferredLanguage>preferredLanguage</preferredLanguage>
 <source>local</source>
 <sourceUserKey>sourceUserKey</sourceUserKey>
 <status>AUTHPENDING</status>
 <suffix>suffix</suffix>
 <surname>surname</surname>
 <timeZone>timeZone</timeZone>
 <title>title</title>
 <userName>userName00</userName>
 <userPassword>userPassword</userPassword>
 <commPassword>commPassword</commPassword>
 <userType>ADMINISTRATOR</userType>
 <commProfileSet>
 <commProfileSetName>
 commProfileSetName00
 </commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="ipt:xmlStationProfile"
 xmlns:ipt="http://xml.avaya.com/schema/import_csm_cm">
 <commProfileType>CM</commProfileType>
 <ipt:cmName>PUIM81</ipt:cmName>
 <ipt:useExistingExtension>
 false
 </ipt:useExistingExtension>

```

```

<ipt:extension>7100000</ipt:extension>
<ipt:template>DEFAULT_4620_CM_6_0</ipt:template>
<ipt:setType>4620</ipt:setType>
<ipt:securityCode>78974231</ipt:securityCode>
<ipt:port>IP</ipt:port>
<ipt:coveragePath1>1</ipt:coveragePath1>
<ipt:tn>1</ipt:tn>
<ipt:cor>10</ipt:cor>
<ipt:cos>4</ipt:cos>
<ipt:dataModule>>false</ipt:dataModule>
<ipt:speakerphone>1-way</ipt:speakerphone>
<ipt:displayLanguage>english</ipt:displayLanguage>
<ipt:ipSoftphone>>false</ipt:ipSoftphone>
<ipt:survivableCOR>internal</ipt:survivableCOR>
<ipt:survivableTrunkDest>
 true
</ipt:survivableTrunkDest>
<ipt:offPremisesStation>
 false
</ipt:offPremisesStation>
<ipt:dataOption>none</ipt:dataOption>
<ipt:displayModule>>false</ipt:displayModule>
<ipt:lwcReception>spe</ipt:lwcReception>
<ipt:lwcActivation>true</ipt:lwcActivation>
<ipt:lwcLogExternalCalls>
 false
</ipt:lwcLogExternalCalls>
<ipt:cdrPrivacy>>false</ipt:cdrPrivacy>
<ipt:redirectNotification>
 true
</ipt:redirectNotification>
<ipt:perButtonRingControl>
 false
</ipt:perButtonRingControl>
<ipt:bridgedCallAlerting>
 false
</ipt:bridgedCallAlerting>
<ipt:bridgedIdleLinePreference>
 false
</ipt:bridgedIdleLinePreference>
<!--
 <ipt:confTransOnPrimaryAppearance>
 </ipt:confTransOnPrimaryAppearance>
 <ipt:customizableLabels>
 </ipt:customizableLabels>
-->
<ipt:expansionModule>true</ipt:expansionModule>
<ipt:ipVideoSoftphone>>false</ipt:ipVideoSoftphone>
<ipt:activeStationRinging>
 single
</ipt:activeStationRinging>
<!--
 <ipt:idleActiveRinging></ipt:idleActiveRinging>
 <ipt:switchhookFlash></ipt:switchhookFlash>
 <ipt:ignoreRotaryDigits></ipt:ignoreRotaryDigits>
-->
<ipt:h320Conversion>>false</ipt:h320Conversion>
<ipt:serviceLinkMode>as-needed</ipt:serviceLinkMode>
<ipt:multimediaMode>enhanced</ipt:multimediaMode>
<!-- <ipt:mwiServedUserType>
 </ipt:mwiServedUserType> -->
<!-- <ipt:audixName></ipt:audixName> -->
<!-- <ipt:automaticMoves></ipt:automaticMoves> -->
<ipt:remoteSoftphoneEmergencyCalls>
 as-on-local

```

```

</ipt:remoteSoftphoneEmergencyCalls>
<!-- <ipt:alwaysUse></ipt:alwaysUse> -->
<ipt:precedenceCallWaiting>
 false
</ipt:precedenceCallWaiting>
<ipt:autoSelectAnyIdleAppearance>
 false
</ipt:autoSelectAnyIdleAppearance>
<ipt:coverageMsgRetrieval>
 true
</ipt:coverageMsgRetrieval>
<ipt:autoAnswer>none</ipt:autoAnswer>
<ipt:dataRestriction>>false</ipt:dataRestriction>
<ipt:idleAppearancePreference>
 false
</ipt:idleAppearancePreference>
<!-- <ipt:attCallWaitingIndication>
 </ipt:attCallWaitingIndication> -->
<!-- <ipt:distinctiveAudibleAlert>
 </ipt:distinctiveAudibleAlert> -->
<ipt:restrictLastAppearance>
 true
</ipt:restrictLastAppearance>
<!-- <ipt:adjunctSupervision></ipt:adjunctSupervision> -->
<!-- <ipt:perStationCpnSendCallingNumber>
 </ipt:perStationCpnSendCallingNumber> -->
<!-- <ipt:busyAutoCallbackWithoutFlash>
 </ipt:busyAutoCallbackWithoutFlash> -->
<ipt:audibleMessageWaiting>
 false
</ipt:audibleMessageWaiting>
<ipt:displayClientRedirection>
 false
</ipt:displayClientRedirection>
<ipt:selectLastUsedAppearance>
 false
</ipt:selectLastUsedAppearance>
<ipt:coverageAfterForwarding>
 s
</ipt:coverageAfterForwarding>
<ipt:directIpIpAudioConnections>
 true
</ipt:directIpIpAudioConnections>
<ipt:ipAudioHairpinning>
 false
</ipt:ipAudioHairpinning>
<!-- <ipt:primeAppearancePreference>
 </ipt:primeAppearancePreference> -->
</commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>
</codeblock>

```

## XML Schema Definition for bulk import of Avaya Breeze® platform profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:smgr="http://xml.avaya.com/schema/import"
 targetNamespace="http://xml.avaya.com/schema/import_ce"
 elementFormDefault="qualified">

 <!-- This is the XML schema for the "CE Profile". It
 defines this profile inside of an XML document that defines

```

```

 a user record (see userimport.xsd) -->

<xsd:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd"/>

<xsd:complexType name="CeCommProfXML">
 <xsd:complexContent>
 <xsd:extension base="smgr:xmlCommProfileType">

 <xsd:sequence>
 <!--
 The following attributes are the names of objects that must
 already be administered in System Manager before performing
 the user import.

 The relative order here cannot be changed because it would
 break backwards compatibility with existing XML documents
 that could be used for an import.
 -->

 <!-- Name of the secondary Session Manager (optional) -->
 <xsd:element name="serviceProfile" type="xsd:string" minOccurs="1" />

 </xsd:sequence>

 </xsd:extension>
</xsd:complexContent>
</xsd:complexType>

</xsd:schema>

```

### Sample XML for bulk import of Avaya Breeze® platform endpoint profiles

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce" xmlns:ns3="http://
xml.avaya.com/schema/import_csm_b5800" xmlns:ns4="http://xml.avaya.com/schema/import1"
xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns6="http://xml.avaya.com/schema/
import_mmcs" xmlns:ns7="http://xml.avaya.com/schema/import_sessionmanager"
xmlns:ns8="http://xml.avaya.com/schema/mock" xmlns:ns9="http://xml.avaya.com/schema/
import_csm_mm" xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm"
xmlns:ns11="http://xml.avaya.com/schema/import_csm_agent" xmlns:ns12="http://
xml.avaya.com/schema/deltaImport" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>basic</authenticationType>
 <description></description>
 <displayName>saurabh, tyagi</displayName>
 <displayNameAscii>saurabh, tyagi</displayNameAscii>
 <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>tyagi</givenName>
 <givenNameAscii>tyagi</givenNameAscii>
 <honorific></honorific>
 <loginName>saurabhtyagi@avaya.com</loginName>
 <employeeNo></employeeNo>
 <department></department>
 <organization></organization>
 <middleName></middleName>
 <preferredLanguage>hu</preferredLanguage>
 <source>local</source>
 <status>provisioned</status>
 <surname>saurabh</surname>
 <surnameAscii>saurabh</surnameAscii>
 <userName>saurabhtyagi</userName>
 </tns:user>

```

```

<userPassword></userPassword>
<roles>
 <role>End-User</role>
</roles>
<ownedContactLists>
 <contactList>
 <name>list-saurabhtyagi_avaya.com</name>
 <isPublic>false</isPublic>
 <contactListType>general</contactListType>
 </contactList>
</ownedContactLists>
<commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="ns2:CeCommProfXML" xmlns:ns2="http://
xml.avaya.com/schema/import_ce">
 <commProfileType>AUS</commProfileType>
 <ns2:serviceProfile>ce_service_profile</ns2:serviceProfile>
 </commProfile>
 </commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema for bulk import and export of Work Assignment profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
 <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:smgr="http://xml.avaya.com/schema/import"
 targetNamespace="http://xml.avaya.com/schema/import_workassignment"
 elementFormDefault="qualified">
 <!-- This is the XML schema for the "Work Assignment Profile". It
 defines this profile inside of an XML document that defines
 a user record (see userimport.xsd) -->
 <xsd:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd" />
 <xsd:complexType name="WorkAssignmentCommProfXML">
 <xsd:complexContent>
 <xsd:extension base="smgr:xmlCommProfileType" />
 <xsd:sequence>
 <xsd:element name="strategyName" type="xsd:string" minOccurs="0"
maxOccurs="1" />
 <xsd:element name="workAssignmentResourceDetails" minOccurs="0"
maxOccurs="unbounded">
 <xsd:complexType>
 <xsd:sequence>
 <xsd:element name="associatedHandleName" type="xsd:string"
minOccurs="1" maxOccurs="1" />
 <xsd:element name="accountName" type="xsd:string" minOccurs="0" maxOccurs="1" />
 <xsd:element name="accountAddress" type="xsd:string" minOccurs="0"
maxOccurs="1" />
 <xsd:element name="sourceName" type="xsd:string" minOccurs="0"
maxOccurs="1" />
 <xsd:element name="sourceAddress" type="xsd:string" minOccurs="0"
maxOccurs="1" />
 <xsd:element name="channelAttribute" type="xsd:string" minOccurs="0"
maxOccurs="1" />
 </xsd:sequence>
 </xsd:complexType>
 </xsd:element>
 <xsd:element name="workAssignmentAgentAttributes" minOccurs="0"
maxOccurs="unbounded">
 <xsd:complexType>
 <xsd:sequence>

```

```

 <xsd:element name="categoryName" type="xsd:string" minOccurs="1"
maxOccurs="1" />
 <xsd:element name="attributeName" type="xsd:string" minOccurs="1"
maxOccurs="1" />
 </xsd:sequence>
</xsd:complexType>
</xsd:element>
</xsd:sequence>
</xsd:extension>
</xsd:complexContent>
</xsd:complexType>
</xsd:schema>

```

## Sample XML for bulk import of Work Assignment profiles

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce" xmlns:tns="http://
xml.avaya.com/schema/import" xmlns:ns4="http://xml.avaya.com/schema/
import_mem officelinx" xmlns:ns5="http://xml.avaya.com/schema/import1"
xmlns:ns6="http://xml.avaya.com/schema/import_csm_mm" xmlns:ns7="http://xml.avaya.com/
schema/import_workassignment" xmlns:ns8="http://xml.avaya.com/schema/
import_sessionmanager" xmlns:ns9="http://xml.avaya.com/schema/presence"
xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns11="http://xml.avaya.com/
schema/import_mmcsc" xmlns:ns12="http://xml.avaya.com/schema/import_csm_b5800"
xmlns:ns13="http://xml.avaya.com/schema/deltaImport" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd">
 <tns:user>
 <UserProvisionRules>
 <UserProvisionRuleName>My UPR Equi</UserProvisionRuleName>
 </UserProvisionRules>
 <authenticationType>basic</authenticationType>
 <description></description>
 <displayName>bbb, aaa</displayName>
 <displayNameAscii>bbb, aaa</displayNameAscii>
 <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>aaa</givenName>
 <givenNameAscii>aaa</givenNameAscii>
 <honorific></honorific>
 <loginName>aaa@avaya.com</loginName>
 <employeeNo></employeeNo>
 <department></department>
 <organization></organization>
 <middleName></middleName>
 <preferredLanguage>it_IT</preferredLanguage>
 <source>local</source>
 <status>provisioned</status>
 <surname>bbb</surname>
 <surnameAscii>bbb</surnameAscii>
 <timeZone>(-12:0)International Date Line West</timeZone>
 <userName>aaa</userName>
 <userPassword></userPassword>
 <commPassword></commPassword>
 <roles>
 <role>End-User</role>
 </roles>
 <ownedContactLists>
 <contactList>
 <name>list-aaa_avaya.com</name>
 <isPublic>false</isPublic>
 <contactListType>general</contactListType>
 </contactList>
 </ownedContactLists>
 </tns:user>

```

```

 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <handleList>
 <handle>
 <handleName>aaa@avaya.com</handleName>
 <handleType>uca</handleType>
 </handle>
 </handleList>
 <commProfileList>
 <commProfile xsi:type="ns7:WorkAssignmentCommProfXML" xmlns:ns7="http://
xml.avaya.com/schema/import_workassignment">
 <commProfileType>UCA</commProfileType>
 <ns7:strategyName>Skill Level</ns7:strategyName>
 <ns7:workAssignmentResourceDetails>
 <ns7:associatedHandleName>aaa@avaya.com</
ns7:associatedHandleName>
 <ns7:accountName>aaa</ns7:accountName>
 <ns7:accountAddress>aaa@avaya.com</ns7:accountAddress>
 <ns7:sourceName>avaya.com</ns7:sourceName>
 <ns7:sourceAddress></ns7:sourceAddress>
 <ns7:channelAttribute>Voice</ns7:channelAttribute>
 </ns7:workAssignmentResourceDetails>
 </commProfile>
 </commProfileList>
 </commProfileSet>
 </tns:user>
</tns:users>

```

## XML Schema Definition for bulk import of Avaya Messaging profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:smgr="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
 targetNamespace="http://xml.avaya.com/schema/import_mem_officelinx">

 <xs:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd" />

 <xs:complexType name="xmlOfficelinxProfile">
 <xs:complexContent>
 <xs:extension base="smgr:xmlCommProfileType">
 <xs:sequence>
 <xs:element type="xs:string" name="officelinxName" maxOccurs="1" />
 <xs:element type="xs:long" name="mailBoxNumber" maxOccurs="1" />
 <xs:element type="xs:string" name="numericPassword" maxOccurs="1"
minOccurs="0" />
 <xs:element type="xs:string" name="applicationUserPassword"
maxOccurs="1" minOccurs="0" />
 <xs:element type="xs:string" name="company" maxOccurs="1"
minOccurs="0" />
 <xs:element type="xs:string" name="department" maxOccurs="1"
minOccurs="0" />
 <xs:element type="xs:string" name="featureGroup" maxOccurs="1"
minOccurs="0" />
 <xs:element type="xs:string" name="capability" maxOccurs="1"
minOccurs="0" />
 <xs:element type="xs:string" name="domainAccountName" maxOccurs="1"
minOccurs="0" />
 <xs:element type="xs:string" name="synchronizationUserName"
maxOccurs="1" minOccurs="0" />
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
 </xs:complexType>

```



```
</xs:schema>
```

## Sample XML for bulk import of Avaya Messaging profiles

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce" xmlns:tns="http://
xml.avaya.com/schema/import" xmlns:ns4="http://xml.avaya.com/schema/
import_mem_officelinx" xmlns:ns5="http://xml.avaya.com/schema/import1"
xmlns:ns6="http://xml.avaya.com/schema/import_csm_mm" xmlns:ns7="http://xml.avaya.com/
schema/import_workassignment" xmlns:ns8="http://xml.avaya.com/schema/
import_sessionmanager" xmlns:ns9="http://xml.avaya.com/schema/presence"
xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm" xmlns:ns11="http://xml.avaya.com/
schema/import_mmcs" xmlns:ns12="http://xml.avaya.com/schema/import_csm_agent"
xmlns:ns13="http://xml.avaya.com/schema/import_csm_b5800" xmlns:ns14="http://
xml.avaya.com/schema/deltaImport" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>basic</authenticationType>
 <description></description>
 <displayName>pp7, pp7</displayName>
 <displayNameAscii>pp7, pp7</displayNameAscii>
 <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>pp7</givenName>
 <givenNameAscii>pp7</givenNameAscii>
 <honorific></honorific>
 <loginName>pp7@avaya.com</loginName>
 <employeeNo></employeeNo>
 <department></department>
 <organization></organization>
 <middleName></middleName>
 <preferredLanguage>sv</preferredLanguage>
 <source>local</source>
 <status>provisioned</status>
 <surname>pp7</surname>
 <surnameAscii>pp7</surnameAscii>
 <userName>pp7</userName>
 <userPassword></userPassword>
 <commPassword></commPassword>
 <roles>
 <role>End-User</role>
 </roles>
 <ownedContactLists>
 <contactList>
 <name>list-pp7_avaya.com</name>
 <isPublic>false</isPublic>
 <contactListType>general</contactListType>
 </contactList>
 </ownedContactLists>
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="ns4:xmlOfficelinxProfile" xmlns:ns4="http://
xml.avaya.com/schema/import_mem_officelinx">
 <commProfileType>officelinx</commProfileType>
 <ns4:officelinxName>Officelinx-Pune</ns4:officelinxName>
 <ns4:mailBoxNumber>198</ns4:mailBoxNumber>
 <ns4:numericPassword/>
 <ns4:applicationUserPassword/>
 <ns4:company>1</ns4:company>
 <ns4:department>14</ns4:department>
 <ns4:featureGroup>1</ns4:featureGroup>
```

```

 <ns4:capability>1</ns4:capability>
 <ns4:domainAccountName>pp7@avaya.com</ns4:domainAccountName>
 <ns4:synchronizationUserName>pp7@avaya.com</
ns4:synchronizationUserName>
 </commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk import of Equinox profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:one="http://
xml.avaya.com/schema/import" targetNamespace="http://xml.avaya.com/schema/
import_scopia" elementFormDefault="qualified" xmlns:abc="http://xml.avaya.com/schema/
import_scopia">
<xsd:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd"/>
<xsd:complexType name="ScopiaCommProfileType">
 <xsd:complexContent>
 <xsd:extension base="one:xmlCommProfileType" >
 <xsd:sequence>
 <xsd:element name="scopiaUserId" type="xsd:string" minOccurs="0"/>
 <xsd:element name="password" type="xsd:string"/>
 <xsd:element name="vrNumber" type="xsd:string" minOccurs="0"/>
 <xsd:element name="needVR" type="xsd:boolean" minOccurs="0"/>
 <xsd:element name="virtualRoomId" type="xsd:string" minOccurs="0"/>
 </xsd:sequence>
 </xsd:extension>
 </xsd:complexContent>
</xsd:complexType>
</xsd:schema>

```

## Sample XML for bulk import of Equinox profiles

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:ns2="http://xml.avaya.com/schema/import_ce" xmlns:tns="http://
xml.avaya.com/schema/import" xmlns:ns4="http://xml.avaya.com/schema/
import_mem_officelinx" xmlns:ns5="http://xml.avaya.com/schema/import1"
xmlns:ns15="http://xml.avaya.com/schema/import_scopia" xmlns:ns6="http://xml.avaya.com/
schema/import_csm_mm" xmlns:ns7="http://xml.avaya.com/schema/import_workassignment"
xmlns:ns8="http://xml.avaya.com/schema/import_sessionmanager" xmlns:ns9="http://
xml.avaya.com/schema/presence" xmlns:ns10="http://xml.avaya.com/schema/import_csm_cm"
xmlns:ns11="http://xml.avaya.com/schema/import_mmcs" xmlns:ns12="http://xml.avaya.com/
schema/import_csm_b5800" xmlns:ns13="http://xml.avaya.com/schema/deltaImport"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>basic</authenticationType>
 <description></description>
 <displayName>Firstname, Lastname</displayName>
 <displayNameAscii>Firstname, Lastname</displayNameAscii>
 <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>Lastname</givenName>
 <givenNameAscii>Lastname</givenNameAscii>
 <honorific></honorific>
 <loginName>abc@avaya.com</loginName>
 <employeeNo></employeeNo>
 <department></department>
 <organization></organization>
 <middleName></middleName>
 <preferredLanguage>pl</preferredLanguage>
 <source>local</source>
 </tns:user>

```

```

<status>provisioned</status>
<surname>Firstname</surname>
<surnameAscii>Firstname</surnameAscii>
<userName>abc</userName>
<userPassword></userPassword>
<commPassword>12345</commPassword>
<roles>
 <role>End-User</role>
</roles>
<ownedContactLists>
 <contactList>
 <name>list-abc_avaya.com</name>
 <isPublic>false</isPublic>
 <contactListType>general</contactListType>
 </contactList>
</ownedContactLists>
<commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="ns15:ScopiaCommProfileType" xmlns:ns15="http://
xml.avaya.com/schema/import_scopia">
 <commProfileType>scopiaProfile</commProfileType>
 <ns15:scopiaUserId>1654</ns15:scopiaUserId>
 <ns15:password>1111</ns15:password>
 <ns15:vrNumber>6985001</ns15:vrNumber>
 <ns15:needVR>true</ns15:needVR>
 <ns15:virtualRoomId>16582</ns15:virtualRoomId>
 </commProfile>
 </commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk import of Messaging profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:one="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
 targetNamespace="http://xml.avaya.com/schema/import_csm_mm" xmlns:csm="http://
xml.avaya.com/schema/import_csm_mm">

 <xs:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd" />
 <!--Changes in xsd file need to generate JAXB src using this xsd-->
 <xs:complexType name="xmlMessagingProfile">
 <xs:complexContent>
 <xs:extension base="one:xmlCommProfileType">
 <xs:sequence>
 <!--
 Specifies the messaging system of the subscriber you
 want to add. Name as it appears under
 'Applications/Application Management/Entities
 -->
 <xs:element name="messagingName" type="xs:string"
 maxOccurs="1" minOccurs="1" />
 <xs:element name="useExisting" type="xs:boolean"
 maxOccurs="1" minOccurs="0" /><!-- use existing -->

 <!-- Specifies the messaging template of a subscriber. -->
 <xs:element name="messagingTemplate" type="xs:string"
 maxOccurs="1" minOccurs="0" />

 <xs:element name="mailboxNumber" maxOccurs="1"

```

```

 minOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{1,50}" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--
 Specifies the default password the subscriber must use
 to log in to his or her mailbox. The password can be
 from one digit in length to a maximum of 15 digits.
 -->
 <xs:element name="password" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{0,15}" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="deleteOnUnassign" type="xs:boolean"
 maxOccurs="1" minOccurs="0" />

 <!-- follows overriding subscriber data -->

 <!--
 The class of service for this subscriber. The COS controls
 subscriber access to many features and provides general
 settings, such as mailbox size.
 -->
 <xs:element name="cos" maxOccurs="1" minOccurs="0">
 <!-- MM/CMM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern
 value="[0-9]|[0-9]{2}|[0-4][0-9]{2}|[5][0-4][0-9] |
[5][5][0-1]" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--
 Specifies the default community ID for the subscriber.
 Community IDs are used to control message sending and
 receiving among groups of subscribers.
 The default value is 1.
 -->
 <xs:element name="communityID" maxOccurs="1" minOccurs="0">
 <!-- MM/CMM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]|[0-1][0-5]" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--
 Specifies the name that appears before the machine name
 and domain in the subscriber's e-mail address. The machine
 name and domain are automatically added to the handle you
 enter when the subscriber sends or receives an e-mail.
 -->
 <xs:element name="emailHandle" maxOccurs="1" minOccurs="0">
 <!-- MM/CMM field -->
 <xs:simpleType>

```

```

 <xs:restriction base="xs:string">
 <xs:pattern value="^[a-zA-Z0-9\\w\\.\\-]*" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Specifies the display name of the subscriber in address book
 listings, such as those for e-mail client applications.
 The name you enter can be 1 to 64 characters in length.
-->
<xs:element name="commonName" type="xs:string"
 maxOccurs="1" minOccurs="0" /> <!-- MM/CMM field -->

<!--
 Specifies one or more alternate number to reach a
 subscriber. You can use secondary extensions to specify
 a telephone number for direct reception of faxes, to
 allow callers to use an existing Caller Application, or
 to identify each line appearance on the subscriber's
 telephone set if they have different telephone numbers.
-->
<xs:element name="secondaryExtension" maxOccurs="1"
 minOccurs="0"> <!-- MM/CMM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{0,50}" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

 <xs:element name="mmSpecific" type="csm:xmlMMSpecific"
 maxOccurs="1" minOccurs="0" />
 <xs:element name="cmmSpecific" type="csm:xmlCMMSpecific"
 maxOccurs="1" minOccurs="0" />
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlMMSpecific">
 <xs:sequence>
 <!--
 Specifies a unique address in the voice mail network. The numeric
 address can be from 1 to 50 digits and can contain the Mailbox
 Number.
 -->
 <xs:element name="numericAddress" maxOccurs="1" minOccurs="0">
 <!-- MM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9])*" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- The primary telephone extension of the subscriber. -->
 <xs:element name="pbxExtension" maxOccurs="1" minOccurs="0">
 <!-- MM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([+0-9])*" />
 </xs:restriction>
 </xs:simpleType>

```

```

</xs:element>

<!--
 The telephone number of the subscriber as displayed in address book
 listings and client applications. The entry can be a maximum of 50
 characters in length and can contain any combination of digits
 (0-9), period (.), hyphen (-), plus sign (+), and left and right
 parentheses ([]) and ({}).
-->
<xs:element name="telephoneNumber" maxOccurs="1"
 minOccurs="0"> <!-- MM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([-+\.()0-9])*" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 If the subscriber name is entered in multi-byte character format,
 then this field specifies the ASCII translation of the subscriber
 name.
-->
<xs:element name="asciiVersionOfName" type="xs:string"
 maxOccurs="1" minOccurs="0" /> <!-- MM field -->

<!--
 Specifies whether your password expires or not. You can choose one
 of the following: - yes: for password to expire - no: if you do not
 want your password to expire
-->
<xs:element name="expirePassword" type="csm:xmlyesNoType"
 maxOccurs="1" minOccurs="0" /> <!-- MM field -->

<!--
 Specifies whether you want your mailbox to be locked. A subscriber
 mailbox can become locked after two unsuccessful login attempts. You
 can choose one of the following: - no: to unlock your mailbox - yes:
 to lock your mailbox and prevent access to it
-->
<xs:element name="mailBoxLocked" type="csm:xmlyesNoType"
 maxOccurs="1" minOccurs="0" /> <!-- MM field -->

<!--
 Specifies the mailbox number or transfer dial string of the
 subscriber's personal operator or assistant. This field also
 indicates the transfer target when a caller to this subscriber
 presses 0 while listening to the subscriber's greeting.
-->
<xs:element name="personalOperatorMailbox" maxOccurs="1"
 minOccurs="0"> <!-- MM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]+([*#],[0-9]+)*" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Specifies when to route calls to the backup operator mailbox. The
 default value for this field is Always Active.
-->
<xs:element name="personalOperatorSchedule" type="xs:string"
 maxOccurs="1" minOccurs="0" /> <!-- MM field -->

```

```

<!--
 Specifies the order in which the subscriber hears the voice
 messages. You can choose one of the following: - urgent first then
 newest: to direct the system to play any messages marked as urgent
 prior to playing non-urgent messages. Both the urgent and non-urgent
 messages are played in the reverse order of how they were received.
 - oldest messages first: to direct the system to play messages in
 the order they were received. - urgent first then oldest: to direct
 the system to play any messages marked as urgent prior to playing
 non-urgent messages. Both the urgent and non-urgent messages are
 played in the order of how they were received. - newest messages
 first: to direct the system to play messages in the reverse order
 of how they were received.
-->
<xs:element name="tuiMessageOrder" maxOccurs="1"
 minOccurs="0"> <!-- MM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="urgent first then newest" />
 <xs:enumeration value="oldest messages first" />
 <xs:enumeration value="newest messages first" />
 <xs:enumeration value="urgent first then oldest" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Specifies the intercom paging settings for a subscriber. You can
 choose one of the following: - paging is off: to disable intercom
 paging for this subscriber. - paging is manual: if the subscriber
 can modify, with Subscriber Options or the TUI, the setting that
 allows callers to page the subscriber. - paging is automatic: if
 the TUI automatically allows callers to page the subscriber.
-->
<xs:element name="intercomPaging" maxOccurs="1" minOccurs="0">
<!-- MM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="paging is off" />
 <xs:enumeration value="paging is manual" />
 <xs:enumeration value="paging is automatic" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Specifies whether a subscriber can receive messages, e-mail messages
 and call-answer messages from other subscribers. You can choose one
 of the following: - yes: to allow the subscriber to create, forward,
 and receive messages. - no: to prevent the subscriber from receiving
 call-answer messages and to hide the subscriber from the telephone
 user interface (TUI). The subscriber cannot use the TUI to access
 the mailbox, and other TUI users cannot address messages to the
 subscriber.
-->
<xs:element name="voiceMailEnabled" type="csm:xmlTrueFalseType"
 maxOccurs="1" minOccurs="0" />

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous1" type="csm:xmlLength51Type"
 maxOccurs="1" minOccurs="0" />

```

```

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous2" type="csm:xmlLength51Type"
 maxOccurs="1" minOccurs="0" />

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous3" type="csm:xmlLength51Type"
 maxOccurs="1" minOccurs="0" />

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous4" type="csm:xmlLength51Type"
 maxOccurs="1" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="xmlCMMSpecific">
 <xs:sequence>

 <!--
 Specifies the number of the switch on which this subscriber's
 extension is administered. You can enter "0" through "99", or leave
 this field blank. - Leave this field blank if the host switch number
 should be used. - Enter a "0" if no message waiting indicators
 should be sent for this subscriber. You should enter 0 when the
 subscriber does not have a phone on any switch in the network.
 -->
 <xs:element name="switchNumber" maxOccurs="1" minOccurs="0">
 <!-- CMM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9][0-9]" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--
 Specifies the Subscriber Account Code. The Subscriber Account Code
 is used to create Call Detail Records on the switch for calls placed
 by the voice ports. The value you enter in this field can contain
 any combination of digits from 0 to 9. If an account code is not
 specified, the system will use the subscriber's mailbox extension as
 the account code.
 -->
 <xs:element name="accountCode" maxOccurs="1" minOccurs="0">
 <!-- CMM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9])*" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--

```



```

 Specifies the number to be used as the default destination for the
 Transfer Out of Messaging feature. You can enter 3 to 10 digits in
 this field depending on the length of the system's extension, or
 leave this field blank.
-->
<xs:element name="coveringExtension" maxOccurs="1"
 minOccurs="0"> <!-- CMM field -->
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{0}|[0-9]{3,10}" />
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous1" type="csm:xmlLength11Type"
 maxOccurs="1" minOccurs="0" />

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous2" type="csm:xmlLength11Type"
 maxOccurs="1" minOccurs="0" />

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous3" type="csm:xmlLength11Type"
 maxOccurs="1" minOccurs="0" />

<!--
 Specifies additional, useful information about a subscriber. Entries
 in this field are for convenience and are not used by the messaging
 system.
-->
<xs:element name="miscellaneous4" type="csm:xmlLength11Type"
 maxOccurs="1" minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:simpleType name="xmlyesNoType">
 <xs:restriction base="xs:string">
 <xs:enumeration value="Yes" />
 <xs:enumeration value="No" />
 </xs:restriction>
</xs:simpleType>

<xs:simpleType name="xmlTrueFalseType">
 <xs:restriction base="xs:string">
 <xs:enumeration value="TRUE" />
 <xs:enumeration value="FALSE" />
 </xs:restriction>
</xs:simpleType>

<xs:simpleType name="xmlLength11Type">
 <xs:restriction base="xs:string">
 <xs:maxLength value="11" />

```

```

 </xs:restriction>
 </xs:simpleType>

 <xs:simpleType name="xmlLength51Type">
 <xs:restriction base="xs:string">
 <xs:maxLength value="51" />
 </xs:restriction>
 </xs:simpleType>
</xs:schema>

```

## Sample XML for bulk import of Messaging profiles

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>BASIC</authenticationType>
 <description>description</description>
 <displayName>displayname</displayName>
 <displayNameAscii>displayNameAscii</displayNameAscii>
 <dn>dn</dn>
 <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>givenName00</givenName>
 <honorific>honorific</honorific>
 <loginName>user00_00xyz@avaya.com</loginName>
 <middleName>middleName</middleName>
 <managerName>managerName</managerName>
 <preferredGivenName>preferredGivenName</preferredGivenName>
 <preferredLanguage>preferredLanguage</preferredLanguage>
 <source>local</source>
 <sourceUserKey>sourceUserKey</sourceUserKey>
 <status>AUTHPENDING</status>
 <suffix>suffix</suffix>
 <surname>surname</surname>
 <timeZone>timeZone</timeZone>
 <title>title</title>
 <userName>userName00</userName>
 <userPassword>userPassword</userPassword>
 <commPassword>commPassword</commPassword>
 <userType>ADMINISTRATOR</userType>
 <commProfileSet>
 <commProfileSetName>
 commProfileSetName00
 </commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="ipt:xmlMessagingProfile"
 xmlns:ipt="http://xml.avaya.com/schema/import_csm_mm">
 <commProfileType>Messaging</commProfileType>
 <ipt:messagingName>MM-155-187</ipt:messagingName>
 <ipt:useExisting>false</ipt:useExisting>
 <ipt:messagingTemplate>
 DEFAULT_MM_5_2
 </ipt:messagingTemplate>
 <ipt:mailboxNumber>3201</ipt:mailboxNumber>
 <ipt:password>534456346</ipt:password>
 <ipt:cos>0</ipt:cos>
 <ipt:communityID>1</ipt:communityID>
 <ipt:mmSpecific>
 <ipt:numericAddress>3201</ipt:numericAddress>
 <ipt:pbxExtension>32134</ipt:pbxExtension>
 <ipt:telephoneNumber>42342</ipt:telephoneNumber>
 </ipt:mmSpecific>
 </commProfile>
 </commProfileList>
 </commProfileSet>
 </tns:user>
</tns:users>

```

```

 <!--<ipt:expirePassword></ipt:expirePassword>-->
 <ipt:tuiMessageOrder>newest messages first
</ipt:tuiMessageOrder>
 <ipt:intercomPaging>paging is off
</ipt:intercomPaging>
 <ipt:voiceMailEnabled>
 FALSE
 </ipt:voiceMailEnabled>
 <ipt:miscellaneous1>
 Miscellaneous
 </ipt:miscellaneous1>
 </ipt:mmSpecific>
 </commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk import of agent profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:one="http://xml.avaya.com/
schema/import" elementFormDefault="qualified"
targetNamespace="http://xml.avaya.com/schema/import_csm_agent" xmlns:csm="http://
xml.avaya.com/schema/import_csm_agent">
<xs:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>

<!--Changes in xsd file need to generate jaxb src using this xsd-->
<xs:complexType name="xmlAgentProfile">
 <xs:complexContent>
 <xs:extension base="one:xmlCommProfileType" >
 <xs:sequence>
 <!-- CM Name as it appears under 'Applications/Application Management/
Entities -->
 <xs:element name="cmName" type="xs:string" maxOccurs="1" minOccurs="1"/>

 <!-- 'true' if already created extension is to be used. 'false' if
available extension is to be used. -->
 <xs:element name="useExistingAgent" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

 <!-- Extension Range which will be used to create Agent using available
extension within given range -->
 <xs:element name="extensionRange" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|([0-9]+([\.\-]
[0-9]+)*:[0-9]+([\.\-][0-9]+)*)"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Agent Login ID extension number that need to be assigned to the
user. -->
 <xs:element name="loginIdExtension" maxOccurs="1" minOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="([0-9]+([\.\-][0-9]+)*)|[nN][eE][xX]
[tT]"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Template name to be used to create agent. Values defined in

```

```

Template will be used if not provided. -->
<xs:element name="template" type="xs:string" maxOccurs="1"
minOccurs="0"/>

 <!-- Security code for station. Value can be digit only. -->
 <xs:element name="securityCode" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{0,4}" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="aas" type="xs:boolean" maxOccurs="1" minOccurs="0"/>
 <xs:element name="audix" type="xs:boolean" maxOccurs="1" minOccurs="0"/>

 <xs:element name="password" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]{0,9}" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="portExtension" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]+([\.\-][0-9]+)*/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!-- Whether the agent should be deleted if it unassigned from the
user. -->
 <xs:element name="deleteOnUnassign" type="xs:boolean" maxOccurs="1"
minOccurs="0"/>

 <!-- CM dependent field for max value -->
 <xs:element name="tn" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="1" />
 <xs:maxInclusive value="250" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="cor" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:int">
 <xs:minInclusive value="0"/>
 <xs:maxInclusive value="995"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <!--Coverage path = Enter path number between 1-9999, time of day table
t1-t999, or blank - CM Dependent-->
 <xs:element name="coveragePath" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="(t[1-9][0-9]{0,2})|([1-9]{0})|([1-9][0-9]
{0,3})"/>
 </xs:restriction>
 </xs:simpleType>

```

```

</xs:element>

<xs:element name="lwcReception" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="audix"/>
 <xs:enumeration value="msa"/>
 <xs:enumeration value="spe"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<xs:element name="lwcLogExternalCalls" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
<xs:element name="audixNameforMessaging" type="xs:string" maxOccurs="1"
minOccurs="0" />
<xs:element name="hearsServiceObservingTone" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
<xs:element name="loginIDforISDNSIPDisplay" type="xs:boolean"
maxOccurs="1" minOccurs="0" />

<xs:element name="autoAnswer" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="acd"/>
 <xs:enumeration value="all"/>
 <xs:enumeration value="none"/>
 <xs:enumeration value="station"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<xs:element name="miaAcrossSkills" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="n"/>
 <xs:enumeration value="y"/>
 <xs:enumeration value="system"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<xs:element name="acwAgentConsideredIdle" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="n"/>
 <xs:enumeration value="y"/>
 <xs:enumeration value="system"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<xs:element name="auxWorkReasonCodeType" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="forced"/>
 <xs:enumeration value="requested"/>
 <xs:enumeration value="system"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>

<xs:element name="logoutReasonCodeType" maxOccurs="1" minOccurs="0">

```

```

 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="forced"/>
 <xs:enumeration value="requested"/>
 <xs:enumeration value="system"/>
 <xs:enumeration value="none"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="maximumTimeAgentInAcwBeforeLogoutSec" maxOccurs="1"
minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|[3-9][0-9]{1}|[1-9][0-9]{1,3}|(none)|
(system)"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="forcedAgentLogoutTimeHr" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|[0-9]|[1][0-9]{1}|[2][0-3]{1}"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="forcedAgentLogoutTimeSec" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|(00)|(15)|(30)|(45)"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="directAgentSkill" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|[1-9]|[1-9][0-9]{0,2}|[1-7][0-9]{3}|
8000"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="callHandlingPreference" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="greatest-need"/>
 <xs:enumeration value="percent-allocation"/>
 <xs:enumeration value="skill-level"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="serviceObjective" type="xs:boolean" maxOccurs="1"
minOccurs="0" />
 <xs:element name="directAgentCallsFirst" type="xs:boolean"
maxOccurs="1" minOccurs="0" />
 <xs:element name="localCallPreference" type="xs:boolean" maxOccurs="1"
minOccurs="0" />

 <xs:element name="skills" type="csm:xmlAgentLoginIdSkillsData"
maxOccurs="unbounded" minOccurs="0" />

```

```

 <xs:element name="nativeName" type="csm:xmlNativeNameData"
maxOccurs="1" minOccurs="0"/>

 <!--

 private String NativeNameScripts;

 -->
 </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="xmlAgentLoginIdSkillsData">
 <xs:sequence>
 <!--
 private AgentLoginIdData agentLoginId;

 -->
 <xs:element name="number" type="xs:string" maxOccurs="1" minOccurs="1" />
 <xs:element name="skillNumber" maxOccurs="1" minOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[1-9][0-9]{0,2}|[1-7][0-9]{3}|8000"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="reserveLevel" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|a|m|n|[1-2]"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="skillLevel" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|[1-9]|[1-9][0-6]{1}"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="percentAllocation" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="|[1-9]|[1-9][0-9]{1}|100"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 </xs:sequence>
</xs:complexType>

<!-- If displayName,givenName or surname contains characters of multiple scripts then
locale tag should be present.
 If displayName tag is present then it overwrites native name.
 If displayname is not present then combination of givenName and surname gets
copied in native name.
Please find below locale for multiscript language
Language Locale
Japanese ja, ja-jp
Simplified Chinese zh-cn

```

```

 Traditional Chinese zh-tw-->
<xs:complexType name="xmlNativeNameData">
 <xs:sequence>
 <xs:element name="locale" maxOccurs="1" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="ja-jp"/>
 <xs:enumeration value="ja"/>
 <xs:enumeration value="zh-cn"/>
 <xs:enumeration value="zh-tw"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 <xs:element name="name" maxOccurs="1" minOccurs="0" >
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="27"/>
 </xs:restriction>
 </xs:simpleType>
 </xs:element>
 </xs:sequence>
</xs:complexType>
</xs:schema>

```

## XML Schema for CS 1000 Communication Profile

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:one="http://xml.avaya.com/schema/import"
 targetNamespace="http://xml.avaya.com/schema/import1"
 elementFormDefault="qualified"
 xmlns:abc="http://xml.avaya.com/schema/import1">
 <xsd:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd"/>
 <xsd:complexType name="AccountCommProfileType">
 <xsd:complexContent>
 <xsd:extension base="one:xmlCommProfileType" >
 <xsd:sequence>
 <xsd:element name="serviceDetails" type="xsd:string" minOccurs="0"/>
 <xsd:element name="element" type="xsd:string" minOccurs="0"/>
 <xsd:element name="target" type="xsd:string" minOccurs="0"/>
 <xsd:element name="template" type="xsd:string" minOccurs="0"/>
 <xsd:element name="serviceType" type="xsd:string" minOccurs="0"/>
 <xsd:element name="accountDetails" type="xsd:string" minOccurs="0"/>
 <xsd:element name="accountProperties" type="abc:AccountPropertyType"
minOccurs="0" maxOccurs="unbounded"/>
 </xsd:sequence>
 </xsd:extension>
 </xsd:complexContent>
 </xsd:complexType>

 <xsd:complexType name="AccountPropertyType">
 <xsd:sequence>
 <xsd:element name="propertyName" type="xsd:string"/>
 <xsd:element name="propertyValue" type="xsd:string"/>
 </xsd:sequence>
 </xsd:complexType>
</xsd:schema>

```

## Sample XML for CS 1000 Communication Profiles

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ns3="http://
xml.avaya.com/schema/import1" xmlns:ns4="http://xml.avaya.com/schema/deltaImport"

```



```

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>basic</authenticationType>
 <description></description>
 <displayName>singleUser, singleUser</displayName>
 <displayNameAscii>singleUser, singleUser</displayNameAscii>
 <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>singleUser</givenName>
 <honorific></honorific>
 <loginName>singleuser@avaya.com</loginName>
 <employeeNo></employeeNo>
 <department></department>
 <organization></organization>
 <middleName></middleName>
 <preferredLanguage>en_US</preferredLanguage>
 <source>local</source>
 <sourceUserKe>Ynone</sourceUserKe>Y
 <status>provisioned</status>
 <surname>singleUser</surname>
 <userName>singleuser</userName>
 <userPassword></userPassword>
 <roles>
 <role>End-User</role>
 </roles>
 <ownedContactLists>
 <contactList>
 <name>list-singleuser_avaya.com</name>
 <description></description>
 <isPublic>false</isPublic>
 <contactListType>general</contactListType>
 </contactList>
 </ownedContactLists>
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimar>Ytrue</isPrimar>Y
 <commProfileList>
 <commProfile xsi:type="ns3:AccountCommProfileType" xmlns:ns3="http://
xml.avaya.com/schema/import1">
 <commProfileType>accountCommProfile</commProfileType>
 <ns3:serviceDetails>DN=8054(Marped), TN=004 0 00 12, TYPE=M2602</
ns3:serviceDetails>
 <ns3:element>CS1K Mock Element Manager</ns3:element>
 <ns3:target>Target1</ns3:target>
 <ns3:template>Premium</ns3:template>
 </ns3:serviceType>com.nortel.ems.services.account.Telephony</ns3:serviceType>
 <ns3:properties>
 <ns3:property name="prefEsn">343-8054</ns3:property>Y
 <ns3:property name="prefDn">8054</ns3:property>Y
 </ns3:properties>
 <ns3:isPublished>true</ns3:isPublished>
 </commProfile>
 </commProfileList>
 </commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema for IP Office Communication Profiles

```

<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:one="http://xml.avaya.com/schema/import" elementFormDefault="qualified"
 targetNamespace="http://xml.avaya.com/schema/import_csm_b5800" xmlns:csm="http://

```

```

xml.avaya.com/schema/import_csm_b5800">

 <xs:import namespace="http://xml.avaya.com/schema/import"
 schemaLocation="userimport.xsd" />

 <!--Changes in xsd file need to generate jaxb src using this xsd-->
 <xs:complexType name="xmlB5800UserProfile">
 <xs:complexContent>
 <xs:extension base="one:xmlCommProfileType">
 <xs:sequence>
 <!--
 IPOffice/B5800/B5800L Device Name as it appears under
'Applications/Application
 Management/Entities
 -->
 <xs:element name="deviceName" type="xs:string" maxOccurs="1"
 minOccurs="1" />

 <!--
 Template name to be used to create station. Values defined in
 Template will be used if not provided.
 -->
 <xs:element name="userTemplate" type="xs:string"
 maxOccurs="1" minOccurs="0" />

 <xs:element name="useExistingExt" type="xs:boolean"
 maxOccurs="1" minOccurs="0" />

 <!-- extension number that need to be assigned to the user. -->
 <xs:element name="extension" maxOccurs="1" minOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:pattern value="[0-9]+([\.\-][0-9]+)*" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="modulePort" type="xs:string"
 maxOccurs="1" minOccurs="0" />

 <!-- Specifies the type of the extn -->
 <xs:element name="extensionType" maxOccurs="1"
 minOccurs="1">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:enumeration value="Analog" />
 <xs:enumeration value="IPDECT" />
 <xs:enumeration value="SIPDECT" />
 <xs:enumeration value="Sip" />
 <xs:enumeration value="Digital" />
 <xs:enumeration value="H323" />
 </xs:restriction>
 </xs:simpleType>
 </xs:element>

 <xs:element name="deleteExtOnUserDelete" type="xs:boolean"
 maxOccurs="1" minOccurs="0" />

 <xs:element name="data" type="csm:xmlB5800UserProfileData"
 maxOccurs="1" minOccurs="0" />
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
 </xs:complexType>

```

```

</xs:complexType>

<xs:complexType name="xmlB5800UserProfileData">
 <xs:sequence>
 <xs:element name="ws_object" type="csm:xmlB5800UserConfig">
 </xs:element>
 </xs:sequence>
 </xs:complexType>

 <xs:complexType name="xmlB5800UserConfig">
 <xs:sequence>
 <xs:element name="Extension" type="csm:xmlB5800ExtensionInfo">
 </xs:element>
 <xs:element name="User" type="csm:xmlB5800UserInfo">
 </xs:element>
 </xs:sequence>
 </xs:complexType>

 <xs:complexType name="xmlB5800ExtensionInfo">
 <xs:sequence>
 <xs:element name="Id" type="xs:int" minOccurs="0" />
 <xs:element name="SubId" type="xs:string" minOccurs="0" />
 <xs:element name="Extension" type="xs:string" minOccurs="0" />
 <xs:element name="TypeInfo" type="xs:int" minOccurs="0" />
 <xs:element name="CallerDisplayType" type="xs:int" minOccurs="0" />
 <xs:element name="MessageLampType" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnClassification" type="xs:int" minOccurs="0" />
 <xs:element name="LineType" type="xs:int" minOccurs="0" />
 <xs:element name="MinFlashPulseWidth" type="xs:int" minOccurs="0" />
 <xs:element name="MaxFlashPulseWidth" type="xs:int" minOccurs="0" />
 <xs:element name="UseSystemFlashHook" type="xs:boolean" minOccurs="0" />
 <xs:element name="ResetVolumeAfterCalls" type="xs:boolean" minOccurs="0" />
 <xs:element name="DisconnectPulseWidth" type="xs:int" minOccurs="0" />
 <xs:element name="HookPersistency" type="xs:int" minOccurs="0" />
 <xs:element name="Mac" type="xs:string" minOccurs="0" />
 <xs:element name="SilenceSuppression" type="xs:boolean" minOccurs="0" />
 <xs:element name="VoicePktSize" type="xs:int" minOccurs="0" />
 <xs:element name="VoiceCompression" type="xs:int" minOccurs="0" />
 <xs:element name="voip" type="csm:xmlVoip" minOccurs="0" />
 <xs:element name="RenegotiationSupported" type="xs:boolean" minOccurs="0" />
 <xs:element name="RenegotiateBeforeConnect" type="xs:boolean"
minOccurs="0" />
 <xs:element name="UseVocoder" type="xs:boolean" minOccurs="0" />
 <xs:element name="EarlyH245Supported" type="xs:boolean" minOccurs="0" />
 <xs:element name="RFC2833" type="xs:boolean" minOccurs="0" />
 <xs:element name="MediaWait" type="xs:boolean" minOccurs="0" />
 <xs:element name="MediaOnOverlap" type="xs:boolean" minOccurs="0" />
 <xs:element name="PauseRequired" type="xs:boolean" minOccurs="0" />
 <xs:element name="PauseOnEndRequired" type="xs:boolean" minOccurs="0" />
 <xs:element name="ParallelH245" type="xs:boolean" minOccurs="0" />
 <xs:element name="AnnexFSupported" type="xs:boolean" minOccurs="0" />
 <xs:element name="PhoneType" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIAudio_setting" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIHeadset_setting" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIContrast" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIRedial_time" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPISpeaker_volume" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIHandsfree_settings" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIRingtone_volume" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIDoor_phone" type="xs:boolean" minOccurs="0" />
 <xs:element name="ExtnAPIHandset_volume" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIRingtone_speed" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIHeadset_volume" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIHeadset_config" type="xs:int" minOccurs="0" />
 <xs:element name="ExtnAPIAlpha_keypad_layout" type="xs:int" minOccurs="0" />

```

```

 <xs:element name="ExtnAPIDirect_dial_enabled" type="xs:boolean"
minOccurs="0" />
 <xs:element name="ExtnAPIHandsfree_enabled" type="xs:boolean"
minOccurs="0" />
 <xs:element name="T38Fax" type="csm:xmlT38Fax" minOccurs="0" />
 <xs:element name="SipExtn" type="csm:xmlSipExtn" minOccurs="0" />
 <xs:element name="DisableSpeaker" type="xs:boolean" minOccurs="0" />
 <xs:element name="VPNExtn" type="xs:boolean" minOccurs="0" />
 <xs:element name="IPAvayaLicenseReserved" type="xs:boolean" minOccurs="0" />
 <xs:element name="IPEndpointsLicenseReserved" type="xs:boolean"
minOccurs="0" />
 <xs:element name="IsExtnCentralized" type="xs:boolean" minOccurs="0" />
 <xs:element name="CentralizedDDINumber" type="xs:string" minOccurs="0" />
 <xs:element name="ExtnDS" type="csm:xmlExtnDS" minOccurs="0" />
 <xs:element name="SpecificBstType" type="xs:int" minOccurs="0" />
 <xs:element name="Location" type="xs:string" minOccurs="0" />
 <xs:element name="PhonePassword" type="xs:string" minOccurs="0" />
 <xs:element name="Module" type="xs:string" minOccurs="0" />
 <xs:element name="Port" type="xs:string" minOccurs="0" />
 <xs:element name="AllowRemoteExtn" type="xs:string" minOccurs="0" />
 <xs:element name="FallbackAsRemoteWorker" type="xs:string" minOccurs="0" />
 <xs:element name="RingVoltageBoost" type="xs:string" minOccurs="0" />
 <xs:element name="RemoteLineNumber" type="xs:string" minOccurs="0" />
 <xs:element name="D100Extn" type="csm:xmlD100Extn" minOccurs="0" />
 </xs:sequence>
 <xs:attribute name="GUID" type="xs:string" />
</xs:complexType>

<xs:complexType name="xmlB5800UserInfo">
 <xs:sequence>
 <xs:element name="EUAuth" type="csm:xmlEUAuth" minOccurs="0" />
 <xs:element name="UserRightsView" type="xs:string" minOccurs="0" />
 <xs:element name="UsingView" type="xs:boolean" minOccurs="0" />
 <xs:element name="UserRightsTimeProfile" type="xs:string" minOccurs="0" />
 <xs:element name="OutOfHoursUserRights" type="xs:string" minOccurs="0" />
 <xs:element name="Name" type="xs:string" minOccurs="0" />
 <xs:element name="KName" type="xs:string" minOccurs="0" />
 <xs:element name="Password" type="xs:string" minOccurs="0" />
 <xs:element name="FullName" type="xs:string" minOccurs="0" />
 <xs:element name="Extension" type="xs:string" minOccurs="0" />
 <xs:element name="Priority" type="xs:int" minOccurs="0" />
 <xs:element name="OutsideCallSeq" type="xs:int" minOccurs="0" />
 <xs:element name="InsideCallSeq" type="xs:int" minOccurs="0" />
 <xs:element name="RingbackCallSeq" type="xs:int" minOccurs="0" />
 <xs:element name="NoAnswerTime" type="xs:int" minOccurs="0" />
 <xs:element name="ForwardOnBusy" type="xs:boolean" minOccurs="0" />
 <xs:element name="BookConferenceWithPM" type="xs:boolean" minOccurs="0" />
 <xs:element name="DisableForwardOnInt" type="xs:boolean" minOccurs="0" />
 <xs:element name="DisableForwardUncondOnInt" type="xs:boolean"
minOccurs="0" />
 <xs:element name="DisableForwardBusyNoAnsOnInt" type="xs:boolean"
minOccurs="0" />
 <xs:element name="VoicemailReception2" type="xs:string" minOccurs="0" />
 <xs:element name="VoicemailReception3" type="xs:string" minOccurs="0" />
 <xs:element name="DSSKeys" type="csm:xmlDSSKeys" minOccurs="0" />
 <xs:element name="InhibitOffSwitchForwarding" type="xs:boolean"
minOccurs="0" />
 <xs:element name="IsNoUser" type="xs:boolean" minOccurs="0" />
 <xs:element name="IsRealUser" type="xs:boolean" minOccurs="0" />
 <xs:element name="IsRemoteManager" type="xs:boolean" minOccurs="0" />
 <xs:element name="IsVoiceEmailModeAlert" type="xs:boolean" minOccurs="0" />
 <xs:element name="IsVoiceEmailModeCopy" type="xs:boolean" minOccurs="0" />
 <xs:element name="IsVoiceEmailModeForward" type="xs:boolean"
minOccurs="0" />
 <xs:element name="IsVoiceEmailModeOff" type="xs:boolean" minOccurs="0" />

```

```

 <xs:element name="MaxTwinnedCalls" type="xs:int" minOccurs="0" />
 <xs:element name="PhoneManagerCallStatusOptions" type="xs:long"
minOccurs="0" />
 <xs:element name="PhoneManagerCloseOptions" type="xs:int" minOccurs="0" />
 <xs:element name="PhoneManagerCanChange" type="xs:boolean" minOccurs="0" />
 <xs:element name="PhoneManagerConfigureOptions" type="xs:int"
minOccurs="0" />
 <xs:element name="PhoneManagerOptions" type="xs:int" minOccurs="0" />
 <xs:element name="PhoneManagerOptionsOriginal" type="xs:int"
minOccurs="0" />
 <xs:element name="PhoneType" type="xs:int" minOccurs="0" />
 <xs:element name="PhoneTypeIndex" type="xs:int" minOccurs="0" />
 <xs:element name="PopupAnswering" type="xs:boolean" minOccurs="0" />
 <xs:element name="PopupExternal" type="xs:boolean" minOccurs="0" />
 <xs:element name="PopupInternal" type="xs:boolean" minOccurs="0" />
 <xs:element name="PopupOutlook" type="xs:boolean" minOccurs="0" />
 <xs:element name="PopupRinging" type="xs:boolean" minOccurs="0" />
 <xs:element name="PopupOptions" type="xs:int" minOccurs="0" />
 <xs:element name="RingDelay" type="xs:int" minOccurs="0" />
 <xs:element name="ShowAccountCodes" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowAllCalls" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowCallStatus" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowCostOfCall" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowIncoming" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowMessages" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowMissed" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowOutgoing" type="xs:boolean" minOccurs="0" />
 <xs:element name="ShowSpeedDials" type="xs:boolean" minOccurs="0" />
 <xs:element name="StartInCompactMode" type="xs:boolean" minOccurs="0" />
 <xs:element name="StayInCompactModeOnIncommingCall" type="xs:boolean"
minOccurs="0" />
 <xs:element name="StayInCompacemodeOnOutgoingCall" type="xs:boolean"
minOccurs="0" />
 <xs:element name="T3AllowThirdPartyFwd" type="xs:boolean" minOccurs="0" />
 <xs:element name="T3ProtectFromThirdPartyFwd" type="xs:boolean"
minOccurs="0" />
 <xs:element name="TwinnedDialDelay" type="xs:int" minOccurs="0" />
 <xs:element name="TwinnedEligibleForForwarded" type="xs:boolean"
minOccurs="0" />
 <xs:element name="TwinnedEligibleForGroup" type="xs:boolean"
minOccurs="0" />
 <xs:element name="TwinnedMobileNumber" type="xs:string" minOccurs="0" />
 <xs:element name="TwinnedTimeProfile" type="xs:string" minOccurs="0" />
 <xs:element name="TwinningNumber" type="xs:string" minOccurs="0" />
 <xs:element name="TwinningType" type="xs:int" minOccurs="0" />
 <xs:element name="TwinningUser" type="xs:string" minOccurs="0" />
 <xs:element name="IsTwinSlave" type="xs:string" minOccurs="0" />
 <xs:element name="IsTwinMaster" type="xs:string" minOccurs="0" />
 <xs:element name="InternalTwinning" type="xs:boolean" minOccurs="0" />
 <xs:element name="MobilityTwinning" type="xs:boolean" minOccurs="0" />
 <xs:element name="TwinnedMobileAnswerGuard" type="xs:string"
minOccurs="0" />
 <xs:element name="AutoRecMailBox" type="xs:string" minOccurs="0" />
 <xs:element name="ManualRecMailBox" type="xs:string" minOccurs="0" />
 <xs:element name="PAServicesEnabled" type="xs:string" minOccurs="0" />
 <xs:element name="AutoRecModeIn" type="xs:string" minOccurs="0" />
 <xs:element name="AutoRecModeOut" type="xs:string" minOccurs="0" />
 <xs:element name="DenyAutoIntercomCalls" type="xs:string" minOccurs="0" />
 <xs:element name="MobileCallControl" type="xs:boolean" minOccurs="0" />
 <xs:element name="SpecificBstType" type="xs:string" minOccurs="0" />
 <xs:element name="ForwardOnNoAnswer" type="xs:boolean" minOccurs="0" />
 <xs:element name="ForwardUnconditional" type="xs:boolean" minOccurs="0" />
 <xs:element name="ForwardHuntGroupCalls" type="xs:boolean" minOccurs="0" />
 <xs:element name="ForwardNumber" type="xs:string" minOccurs="0" />
 <xs:element name="ForwardBusyNumber" type="xs:string" minOccurs="0" />

```

```

<xs:element name="DoNotDisturb" type="xs:boolean" minOccurs="0" />
<xs:element name="DNDEExceptions" type="xs:string" minOccurs="0" />
<xs:element name="OutgoingCallBar" type="xs:boolean" minOccurs="0" />
<xs:element name="IncomingCallBar" type="xs:boolean" minOccurs="0" />
<xs:element name="OffHookStation" type="xs:boolean" minOccurs="0" />
<xs:element name="BusyOnHeld" type="xs:boolean" minOccurs="0" />
<xs:element name="FollowMeNumber" type="xs:string" minOccurs="0" />
<xs:element name="CallWaitingOn" type="xs:boolean" minOccurs="0" />
<xs:element name="VoicemailOn" type="xs:boolean" minOccurs="0" />
<xs:element name="VoicemailHelp" type="xs:boolean" minOccurs="0" />
<xs:element name="VoicemailCode" type="xs:string" minOccurs="0" />
<xs:element name="VoicemailEmail" type="xs:string" minOccurs="0" />
<xs:element name="VoicemailEmailReading" type="xs:boolean" minOccurs="0" />
<xs:element name="VoicemailReception" type="xs:string" minOccurs="0" />
<xs:element name="VoicemailEmailMode" type="xs:int" minOccurs="0" />
<xs:element name="VoicemailRingback" type="xs:boolean" minOccurs="0" />
<xs:element name="ShortCodes" type="csm:xmlShortCodes" minOccurs="0" />
<xs:element name="DialInOn" type="xs:boolean" minOccurs="0" />
<xs:element name="DialInTimeProfile" type="xs:string" minOccurs="0" />
<xs:element name="DialInFirewallProfile" type="xs:string" minOccurs="0" />
<xs:element name="SourceNumbers" type="xs:string" minOccurs="0" />
<xs:element name="DialInQuotaTime" type="xs:int" minOccurs="0" />
<xs:element name="LoginCode" type="xs:string" minOccurs="0" />
<xs:element name="LoginIdleTime" type="xs:string" minOccurs="0" />
<xs:element name="WrapUpTime" type="xs:int" minOccurs="0" />
<xs:element name="TwinMaster" type="xs:string" minOccurs="0" />
<xs:element name="SecTwinCallEnabled" type="xs:boolean" minOccurs="0" />
<xs:element name="CanIntrude" type="xs:boolean" minOccurs="0" />
<xs:element name="CannotBeIntruded" type="xs:boolean" minOccurs="0" />
<xs:element name="XDirectory" type="xs:boolean" minOccurs="0" />
<xs:element name="ForceLogin" type="xs:boolean" minOccurs="0" />
<xs:element name="ForceAuthCode" type="xs:boolean" minOccurs="0" />
<xs:element name="ForceAccountCode" type="xs:boolean" minOccurs="0" />
<xs:element name="SystemPhone" type="xs:int" minOccurs="0" />
<xs:element name="AbsentMsg" type="xs:int" minOccurs="0" />
<xs:element name="AbsentSet" type="xs:int" minOccurs="0" />
<xs:element name="AbsentText" type="xs:string" minOccurs="0" />
<xs:element name="T3HuntGroupMembershipStatus" type="xs:string"
minOccurs="0" />
<xs:element name="T3HuntGroupServiceStatus" type="xs:string"
minOccurs="0" />
<xs:element name="T3HuntGroupNightServiceStatus" type="xs:string"
minOccurs="0" />
<xs:element name="T3DirectoryEntries" type="xs:string" minOccurs="0" />
<xs:element name="MonitorGroup" type="xs:string" minOccurs="0" />
<xs:element name="DisplayLocale" type="xs:string" minOccurs="0" />
<xs:element name="Locale" type="xs:string" minOccurs="0" />
<xs:element name="PMType" type="xs:int" minOccurs="0" />
<xs:element name="InboundAutoRecord" type="xs:int" minOccurs="0" />
<xs:element name="OutboundAutoRecord" type="xs:int" minOccurs="0" />
<xs:element name="AutoRecordTimeProfile" type="xs:string" minOccurs="0" />
<xs:element name="RemoteWorker" type="xs:boolean" minOccurs="0" />
<xs:element name="CanAcceptCollectCalls" type="xs:boolean" minOccurs="0" />
<xs:element name="UserRights" type="xs:string" minOccurs="0" />
<xs:element name="Secretaries" type="xs:string" minOccurs="0" />
<xs:element name="TransferReturnTime" type="xs:string" minOccurs="0" />
<xs:element name="AnswerCallWaiting" type="xs:boolean" minOccurs="0" />
<xs:element name="RingingLinePreference" type="xs:boolean" minOccurs="0" />
<xs:element name="IdleLinePreference" type="xs:boolean" minOccurs="0" />
<xs:element name="CoverageTime" type="xs:int" minOccurs="0" />
<xs:element name="AutoVRL" type="xs:int" minOccurs="0" />
<xs:element name="ManualVRL" type="xs:int" minOccurs="0" />
<xs:element name="DelayedRingPreference" type="xs:boolean" minOccurs="0" />
<xs:element name="AnswerPreSelect" type="xs:boolean" minOccurs="0" />
<xs:element name="ReserveLastCA" type="xs:boolean" minOccurs="0" />

```



```

<xs:element name="CallTracingOn" type="xs:boolean" minOccurs="0" />
<xs:element name="DisplayCharges" type="xs:boolean" minOccurs="0" />
<xs:element name="MarkUpFactor" type="xs:int" minOccurs="0" />
<xs:element name="reset_longest_idle_info" type="xs:int" minOccurs="0" />
<xs:element name="NoAnswerStatus" type="xs:int" minOccurs="0" />
<xs:element name="PBXAddress" type="xs:string" minOccurs="0" />
<xs:element name="SIPName" type="xs:string" minOccurs="0" />
<xs:element name="SIPDisplayName" type="xs:string" minOccurs="0" />
<xs:element name="SIPContact" type="xs:string" minOccurs="0" />
<xs:element name="SIPAnonymous" type="xs:boolean" minOccurs="0" />
<xs:element name="AbbreviatedRing" type="xs:boolean" minOccurs="0" />
<xs:element name="CustomerServiceRep" type="xs:boolean" minOccurs="0" />
<xs:element name="ACWTime" type="xs:int" minOccurs="0" />
<xs:element name="AutoACW" type="xs:boolean" minOccurs="0" />
<xs:element name="UMSWebServices" type="xs:boolean" minOccurs="0" />
<xs:element name="DisableVMOnFU" type="xs:boolean" minOccurs="0" />
<xs:element name="DTMFCallCtrl" type="xs:boolean" minOccurs="0" />
<xs:element name="LoggedOutTwinning" type="xs:int" minOccurs="0" />
<xs:element name="OneXClient" type="xs:boolean" minOccurs="0" />
<xs:element name="MobilityFeatures" type="xs:boolean" minOccurs="0" />
<xs:element name="TwinnedBridgeAppearances" type="xs:boolean"
minOccurs="0" />
<xs:element name="TwinnedCoverageAppearances" type="xs:boolean"
minOccurs="0" />
<xs:element name="TwinnedLineAppearances" type="xs:boolean" minOccurs="0" />
<xs:element name="PersonalDirectory" type="xs:string" minOccurs="0" />
<xs:element name="ForwardToVoicemail" type="xs:boolean" minOccurs="0" />
<xs:element name="CoverageGroup" type="xs:string" minOccurs="0" />
<xs:element name="CanChangeHGOOSGroup" type="xs:string" minOccurs="0" />
<xs:element name="CanChangeHGONGroup" type="xs:string" minOccurs="0" />
<xs:element name="IncludeForwardInMenu" type="xs:boolean" minOccurs="0" />
<xs:element name="CallLoggingCentralised" type="xs:string" minOccurs="0" />
<xs:element name="AttentionRing" type="xs:string" minOccurs="0" />
<xs:element name="CoverageRing" type="xs:string" minOccurs="0" />
<xs:element name="LogMissedCallsForHG" type="xs:string" minOccurs="0" />
<xs:element name="DisableForwardToVoicemail" type="xs:int" minOccurs="0" />
<xs:element name="AnnouncementsOn" type="xs:boolean" minOccurs="0" />
<xs:element name="FollowAnnouncementsOn" type="xs:boolean" minOccurs="0" />
<xs:element name="LoopAnnouncementsOn" type="xs:boolean" minOccurs="0" />
<xs:element name="SyncAnnouncementsOn" type="xs:boolean" minOccurs="0" />
<xs:element name="FirstAnnTime" type="xs:int" minOccurs="0" />
<xs:element name="SecondAnnTime" type="xs:int" minOccurs="0" />
<xs:element name="BetweenAnnTime" type="xs:int" minOccurs="0" />
<xs:element name="PostAnnTone" type="xs:int" minOccurs="0" />
<xs:element name="PortalServices" type="xs:int" minOccurs="0" />
<xs:element name="WorkingHoursUserRightsGroup" type="xs:string"
minOccurs="0" />
<xs:element name="T3SelfAdmin" type="xs:string" minOccurs="0" />
<xs:element name="MobileCallback" type="xs:boolean" minOccurs="0" />
<xs:element name="Receptionist" type="xs:boolean" minOccurs="0" />
<xs:element name="SoftPhone" type="xs:boolean" minOccurs="0" />
<xs:element name="OneXTelecommuter" type="xs:boolean" minOccurs="0" />
<xs:element name="AssignedPackage" type="xs:int" minOccurs="0" />
<xs:element name="AutoRecMode" type="xs:int" minOccurs="0" />
<xs:element name="CallLogTimeout" type="xs:string" minOccurs="0" />
<xs:element name="UserCLI" type="xs:string" minOccurs="0" />
<xs:element name="FlareEnabled" type="xs:boolean" minOccurs="0" />
<xs:element name="FlareMode" type="xs:int" minOccurs="0" />
<xs:element name="AutoIntDeny" type="xs:boolean" minOccurs="0" />
<xs:element name="TUIUser" type="csm:xmlTUIUser" minOccurs="0" />
<xs:element name="UserPasswordStatus" type="xs:int" minOccurs="0" />
<xs:element name="BlockForwarding" type="xs:boolean" minOccurs="0" />
<xs:element name="ParkAndPageInfo" type="csm:xmlParkAndPageInfo"
minOccurs="0" />
<xs:element name="MobileVoIPClientEnabled" type="xs:boolean"

```

```

minOccurs="0" />
 <xs:element name="SendMobilityEmail" type="xs:boolean" minOccurs="0" />
 <xs:element name="IPOCCAgent" type="xs:boolean" minOccurs="0" />
 <xs:element name="AgentType" type="xs:string" minOccurs="0" />
 <xs:element name="WebCollaboration" type="xs:boolean" minOccurs="0" />
 <xs:element name="ConferencePIN" type="xs:string" minOccurs="0" />
 </xs:sequence>
 <xs:attribute name="GUID" type="xs:string" />
</xs:complexType>

<xs:complexType name="xmlDSSKeys">
 <xs:sequence>
 <xs:element minOccurs="0" maxOccurs="unbounded" name="DSSKey"
 type="csm:xmlDSSKey"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlDSSKey">
 <xs:sequence>
 <xs:element name="KeyType" type="xs:int" minOccurs="0"/>
 <xs:element name="Label" type="xs:string" minOccurs="0" />
 <xs:element name="ActionObject" type="xs:string" minOccurs="0" />
 <xs:element name="Data" type="xs:string" minOccurs="0" />
 <xs:element name="RingDelay" type="xs:int" minOccurs="0" />
 <xs:element name="IdlePos" type="xs:string" minOccurs="0"/>
 </xs:sequence>
 <xs:attribute name="Key" type="xs:int" />
</xs:complexType>

<xs:complexType name="xmlShortCodes">
 <xs:sequence>
 <xs:element minOccurs="0" maxOccurs="unbounded" name="ShortCode"
 type="csm:xmlShortCode" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlShortCode">
 <xs:sequence>
 <xs:element name="Code" type="xs:string" minOccurs="0" />
 <xs:element name="TelephoneNumber" type="xs:string" minOccurs="0" />
 <xs:element name="LineGroupId" type="xs:int" minOccurs="0" />
 <xs:element name="Feature" type="xs:string" minOccurs="0" />
 <xs:element name="Locale" type="xs:string" minOccurs="0" />
 <xs:element name="ForceAccountCode" type="xs:boolean" minOccurs="0" />
 <xs:element name="ForceAuthCode" type="xs:boolean" minOccurs="0" />
 </xs:sequence>
 <xs:attribute name="GUID" type="xs:string" />
</xs:complexType>

<xs:complexType name="xmlVoip">
 <xs:sequence>
 <xs:element name="GatekeeperPrimaryIPAddress" type="xs:string"
minOccurs="0" />
 <xs:element name="GatekeeperSecondaryIPAddress" type="xs:string"
minOccurs="0" />
 <xs:element name="IPAddress" type="xs:string" minOccurs="0" />
 <xs:element name="EnableFaststart" type="xs:boolean" minOccurs="0" />
 <xs:element name="FaxTransportSupport" type="xs:boolean" minOccurs="0" />
 <xs:element name="FaxTransportMethod" type="xs:int" minOccurs="0" />
 <xs:element name="CodecLockdown" type="xs:boolean" minOccurs="0" />
 <xs:element name="LocalHoldMusic" type="xs:boolean" minOccurs="0" />
 <xs:element name="LocalTones" type="xs:boolean" minOccurs="0" />
 </xs:sequence>

```



```

<xs:element name="RSVPEnabled" type="xs:boolean" minOccurs="0" />
<xs:element name="OOB_DTMF" type="xs:boolean" minOccurs="0" />
<xs:element name="AllowDirectMedia" type="xs:boolean" minOccurs="0" />
<xs:element name="H450Support" type="xs:int" minOccurs="0" />
<xs:element name="Annex1Support" type="xs:boolean" minOccurs="0" />
<xs:element name="InputGain" type="xs:int" minOccurs="0" />
<xs:element name="OutputGain" type="xs:int" minOccurs="0" />
<xs:element name="MediaSecurity" type="xs:int" minOccurs="0" />
<xs:element name="RTP_Authentication" type="xs:boolean" minOccurs="0" />
<xs:element name="RTP_Encryption" type="xs:boolean" minOccurs="0" />
<xs:element name="RTCP_Authentication" type="xs:boolean" minOccurs="0" />
<xs:element name="RTCP_Encryption" type="xs:boolean" minOccurs="0" />
<xs:element name="SRTP_Window_Size" type="xs:string" minOccurs="0" />
<xs:element name="Crypto_Suite_SHA_80" type="xs:boolean" minOccurs="0" />
<xs:element name="Crypto_Suite_SHA_32" type="xs:boolean" minOccurs="0" />
<xs:element name="CodecSelection" type="xs:string" minOccurs="0" />
<xs:element name="SupplementaryServices" type="xs:int" minOccurs="0" />
<xs:element name="DTMFSupport" type="xs:int" minOccurs="0" />
<xs:element name="ReinviteSupported" type="xs:boolean" minOccurs="0" />
<xs:element name="IsMediaSecurityCustom" type="xs:boolean" minOccurs="0" />
<xs:element name="UseAdvancedCodecPrefs" type="xs:boolean" minOccurs="0" />
<xs:element name="AdvancedCodecPrefs" type="csm:xmlAdvancedCodecPrefs"
minOccurs="0" />
</xs:sequence>
</xs:complexType>

<xs:complexType name="xmlSipExtn">
 <xs:sequence>
 <xs:element name="ForceAuthentication" type="xs:boolean" minOccurs="0" />
 <xs:element name="Rel100Supported" type="xs:string" minOccurs="0" />
 <xs:element name="T38Fax" type="csm:xmlT38Fax" minOccurs="0" />
 <xs:element name="SIP3rdPartyAutoAnswer" type="xs:string" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlExtnDS">
 <xs:sequence>
 <xs:element name="AdmmUseHandsetConfig" type="xs:boolean" minOccurs="0" />
 <xs:element name="AdmmType" type="xs:int" minOccurs="0" />
 <xs:element name="AdmmIpei" type="xs:int" minOccurs="0" />
 <xs:element name="AdmmAnonymous" type="xs:boolean" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlT38Fax">
 <xs:sequence>
 <xs:element name="Defaulted" type="xs:string" minOccurs="0" />
 <xs:element name="T38FaxVersion" type="xs:string" minOccurs="0" />
 <xs:element name="RedundancyLowSpeed" type="xs:string" minOccurs="0" />
 <xs:element name="RedundancyHighSpeed" type="xs:string" minOccurs="0" />
 <xs:element name="NSFOVERRIDE" type="xs:string" minOccurs="0" />
 <xs:element name="NSFCountryCode" type="xs:string" minOccurs="0" />
 <xs:element name="NSFVendorCode" type="xs:string" minOccurs="0" />
 <xs:element name="TxNetworkTimeout" type="xs:string" minOccurs="0" />
 <xs:element name="ScanLineFixup" type="xs:string" minOccurs="0" />
 <xs:element name="TopEnhancement" type="xs:string" minOccurs="0" />
 <xs:element name="DisableT30ECM" type="xs:string" minOccurs="0" />
 <xs:element name="DisableT30MR" type="xs:string" minOccurs="0" />
 <xs:element name="DisableEFlagsForFirstDis" type="xs:string"
minOccurs="0" />
 <xs:element name="EflagStartTimer" type="xs:string" minOccurs="0" />
 <xs:element name="EflagStopTimer" type="xs:string" minOccurs="0" />
 <xs:element name="FaxTransport" type="xs:string" minOccurs="0" />
 <xs:element name="TCFMethod" type="xs:int" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

```

```

 <xs:element name="MaxFaxRate" type="xs:int" minOccurs="0" />
 <xs:element name="G711FaxEcanEnabled" type="xs:string" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlD100Extn">
 <xs:sequence>
 <xs:element name="ForceAuthentication" type="xs:boolean" minOccurs="0" />
 <xs:element name="RemoteLineNumber" type="xs:int" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlTUIUser">
 <xs:sequence>
 <xs:element name="TUIFeaturesMenuControls" type="xs:boolean"
minOccurs="0" />
 <xs:element name="TUIFeaturesMenu" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUIBasicCallFunctions" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUIAdvancedCallFunctions" type="xs:boolean"
minOccurs="0" />
 <xs:element name="TUIHotDeskFunctions" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUIPasscodeChange" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUIPhoneLock" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUISelfAdmin" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUIVoiceMailControls" type="xs:boolean" minOccurs="0" />
 <xs:element name="TUIForwarding" type="xs:boolean" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlParkAndPageInfo">
 <xs:sequence>
 <xs:element name="ParkAndPage" type="csm:xmlParkAndPage" minOccurs="0"
maxOccurs="unbounded" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlParkAndPage">
 <xs:sequence>
 <xs:element name="ParkAndPageId" type="xs:string" minOccurs="0" />
 <xs:element name="PagingNumber" type="xs:string" minOccurs="0" />
 <xs:element name="CentrexTransferNumber" type="xs:string" minOccurs="0" />
 <xs:element name="PNPFallBackNumber" type="xs:string" minOccurs="0" />
 <xs:element name="RetryTimeout" type="xs:string" minOccurs="0" />
 <xs:element name="RetryCount" type="xs:string" minOccurs="0" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlAdvancedCodecPrefs">
 <xs:sequence>
 <xs:element name="CodecPref" type="xs:string" minOccurs="0"
maxOccurs="unbounded" />
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlEUAuth">
 <xs:sequence>
 <xs:element type="xs:string" name="EUAAEnable"/>
 <xs:element type="xs:string" name="EUAName"/>
 <xs:element type="xs:string" name="EUAPassword"/>
 <xs:element type="xs:string" name="EUAFullName"/>
 <xs:element type="xs:string" name="EUAExtension"/>
 <xs:element type="xs:string" name="EUALocale"/>
 <xs:element type="xs:string" name="EUADoNotDisturb"/>
 <xs:element type="xs:string" name="EUADNDExceptions"/>
 <xs:element type="xs:string" name="EUAVoicemailOn"/>
 </xs:sequence>
</xs:complexType>

```

```

<xs:element type="xs:string" name="EUAVoicemailCode"/>
<xs:element type="xs:string" name="EUAVoicemailEmail"/>
<xs:element type="xs:string" name="EUAVoicemailEmailMode"/>
<xs:element type="xs:string" name="EUAMobilityTwinning"/>
<xs:element type="xs:string" name="EUATwinningMobileNumber"/>
<xs:element type="xs:string" name="EUALoginCode"/>
<xs:element type="xs:string" name="EUADenyAutoIntercomCalls"/>
<xs:element type="xs:string" name="EUAPersonalDirectory"/>
<xs:element type="xs:string" name="EUAShortCodes"/>
<xs:element type="xs:string" name="EUABlockForwarding"/>
<xs:element type="xs:string" name="EUAFowardNumber"/>
<xs:element type="xs:string" name="EUAFowardBusyNumber"/>
<xs:element type="xs:string" name="EUAFowardOnBusy"/>
<xs:element type="xs:string" name="EUAFowardOnNoAnswer"/>
<xs:element type="xs:string" name="EUADSSKeys"/>
<xs:element type="xs:string" name="EUAVoicemailRingback"/>
<xs:element type="xs:string" name="EUAConferencePIN"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

## Sample XML for the IP Office Communication Profiles

```

<?xml version="1.0" encoding="utf-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
 <tns:user>
 <authenticationType>basic</authenticationType>
 <givenName>test09</givenName>
 <loginName>test09@avaya.com</loginName>
 <middleName />
 <surname>test09</surname>
 <userPassword/>
 <commPassword />
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <commProfileList>
 <commProfile xsi:type="csm:xmlB5800UserProfile" xmlns:csm="http://xml.avaya.com/schema/import_csm_b5800">
 <commProfileType>IP Office</commProfileType>
 <csm:deviceName>Sanjeet_IPO</csm:deviceName>
 <csm:useExistingExt>true</csm:useExistingExt>
 <csm:extension>207</csm:extension>
 <csm:extensionType>Digital</csm:extensionType>
 <csm:deleteExtOnUserDelete>true</csm:deleteExtOnUserDelete>
 <csm:data>
 <csm:ws_object>
 <csm:Extension>
 <csm:Id>1</csm:Id>
 <csm:SubId>0</csm:SubId>
 <csm:Extension>207</csm:Extension>
 <csm:TypeInfo>15</csm:TypeInfo>
 <csm:CallerDisplayType>1</csm:CallerDisplayType>
 <csm:MessageLampType>4</csm:MessageLampType>
 <csm:ExtnClassification>0</csm:ExtnClassification>
 <csm:LineType>6</csm:LineType>
 <csm:MinFlashPulseWidth>2</csm:MinFlashPulseWidth>
 <csm:MaxFlashPulseWidth>50</csm:MaxFlashPulseWidth>
 <csm:UseSystemFlashHook>true</csm:UseSystemFlashHook>
 <csm:ResetVolumeAfterCalls>false</csm:ResetVolumeAfterCalls>
 <csm:DisconnectPulseWidth>80</csm:DisconnectPulseWidth>
 <csm:HookPersistency>100</csm:HookPersistency>
 </csm:Extension>
 </csm:ws_object>
 </csm:data>
 </commProfile>
 </commProfileList>
 </commProfileSet>
 </tns:user>
</tns:users>

```

```

 <csm:Mac>000000000000</csm:Mac>
 <csm:SilenceSuppression>>false</csm:SilenceSuppression>
 <csm:VoicePktSize>160</csm:VoicePktSize>
 <csm:VoiceCompression>0</csm:VoiceCompression>
 <csm:voip>
 <csm:GatekeeperPrimaryIPAddress>0.0.0.0</
csm:GatekeeperPrimaryIPAddress>
 <csm:GatekeeperSecondaryIPAddress>0.0.0.0</
csm:GatekeeperSecondaryIPAddress>
 <csm:IPAddress>0.0.0.0</csm:IPAddress>
 <csm:EnableFaststart>>false</csm:EnableFaststart>
 <csm:FaxTransportSupport>>false</csm:FaxTransportSupport>
 <csm:FaxTransportMethod>3</csm:FaxTransportMethod>
 <csm:CodecLockdown>>false</csm:CodecLockdown>
 <csm:LocalHoldMusic>>false</csm:LocalHoldMusic>
 <csm:LocalTones>>false</csm:LocalTones>
 <csm:RSVPEnabled>>false</csm:RSVPEnabled>
 <csm:OOB_DTMF>true</csm:OOB_DTMF>
 <csm:AllowDirectMedia>true</csm:AllowDirectMedia>
 <csm:H450Support>2</csm:H450Support>
 <csm:Annex1Support>>false</csm:Annex1Support>
 <csm:InputGain>0</csm:InputGain>
 <csm:OutputGain>0</csm:OutputGain>
 <csm:MediaSecurity>0</csm:MediaSecurity>
 <csm:RTP_Authentication>true</csm:RTP_Authentication>
 <csm:RTP_Encryption>true</csm:RTP_Encryption>
 <csm:RTCP_Authentication>true</csm:RTCP_Authentication>
 <csm:RTCP_Encryption>false</csm:RTCP_Encryption>
 <csm:SRTP_Window_Size>64</csm:SRTP_Window_Size>
 <csm:Crypto_Suite_SHA_80>true</csm:Crypto_Suite_SHA_80>
 <csm:Crypto_Suite_SHA_32>>false</csm:Crypto_Suite_SHA_32>
 <csm:CodecSelection>SystemDefault</csm:CodecSelection>
 <csm:SupplementaryServices>2</csm:SupplementaryServices>
 <csm:DTMFSupport>2</csm:DTMFSupport>
 <csm:ReinviteSupported>true</csm:ReinviteSupported>
 <csm:IsMediaSecurityCustom>>false</csm:IsMediaSecurityCustom>
 </csm:voip>
 <csm:RenegotiationSupported>true</csm:RenegotiationSupported>
 <csm:RenegotiateBeforeConnect>>false</csm:RenegotiateBeforeConnect>
 <csm:UseVocoder>>false</csm:UseVocoder>
 <csm:EarlyH245Supported>>false</csm:EarlyH245Supported>
 <csm:RFC2833>false</csm:RFC2833>
 <csm:MediaWait>false</csm:MediaWait>
 <csm:MediaOnOverlap>false</csm:MediaOnOverlap>
 <csm:PauseRequired>false</csm:PauseRequired>
 <csm:PauseOnEndRequired>false</csm:PauseOnEndRequired>
 <csm:ParallelH245>false</csm:ParallelH245>
 <csm:AnnexFSupported>false</csm:AnnexFSupported>
 <csm:PhoneType>47</csm:PhoneType>
 <csm:ExtnAPIAudio_setting>0</csm:ExtnAPIAudio_setting>
 <csm:ExtnAPIHeadset_setting>0</csm:ExtnAPIHeadset_setting>
 <csm:ExtnAPIContrast>0</csm:ExtnAPIContrast>
 <csm:ExtnAPIRedial_time>0</csm:ExtnAPIRedial_time>
 <csm:ExtnAPISpeaker_volume>0</csm:ExtnAPISpeaker_volume>
 <csm:ExtnAPIHandsfree_settings>0</csm:ExtnAPIHandsfree_settings>
 <csm:ExtnAPIRingtone_volume>0</csm:ExtnAPIRingtone_volume>
 <csm:ExtnAPIDoor_phone>false</csm:ExtnAPIDoor_phone>
 <csm:ExtnAPIHandset_volume>0</csm:ExtnAPIHandset_volume>
 <csm:ExtnAPIRingtone_speed>0</csm:ExtnAPIRingtone_speed>
 <csm:ExtnAPIHeadset_volume>0</csm:ExtnAPIHeadset_volume>
 <csm:ExtnAPIHeadset_config>0</csm:ExtnAPIHeadset_config>
 <csm:ExtnAPIAlpha_keypad_layout>0</csm:ExtnAPIAlpha_keypad_layout>
 <csm:ExtnAPIDirect_dial_enabled>false</csm:ExtnAPIDirect_dial_enabled>
 <csm:ExtnAPIHandsfree_enabled>false</csm:ExtnAPIHandsfree_enabled>
 <csm:DisableSpeaker>false</csm:DisableSpeaker>

```

```

<csm:VPNExtn>false</csm:VPNExtn>
<csm:IPAvayaLicenseReserved>false</csm:IPAvayaLicenseReserved>
<csm:IPEndpointsLicenseReserved>false</csm:IPEndpointsLicenseReserved>
<csm:IsExtnCentralized>false</csm:IsExtnCentralized>
<csm:CentralizedDDINumber>||||</csm:CentralizedDDINumber>
<csm:SpecificBstType>-1</csm:SpecificBstType>
<csm:Location>1</csm:Location>
<csm:PhonePassword />
<csm:Module></csm:Module>
<csm:Port></csm:Port>
<csm:AllowRemoteExtn>false</csm:AllowRemoteExtn>
<csm:FallbackAsRemoteWorker>0</csm:FallbackAsRemoteWorker>
<csm:RingVoltageBoost>0</csm:RingVoltageBoost>
<csm:RemoteLineNumber>-1</csm:RemoteLineNumber>
</csm:Extension>
<csm:User>
 <csm:EUAAuth>
 <csm:EUAEnable>0</csm:EUAEnable>
 <csm:EUAName>0</csm:EUAName>
 <csm:EUAPassword>0</csm:EUAPassword>
 <csm:EUAFullName>0</csm:EUAFullName>
 <csm:EUAExtension>0</csm:EUAExtension>
 <csm:EUALocale>0</csm:EUALocale>
 <csm:EUADoNotDisturb>0</csm:EUADoNotDisturb>
 <csm:EUAADNExceptions>0</csm:EUAADNExceptions>
 <csm:EUAVoicemailOn>0</csm:EUAVoicemailOn>
 <csm:EUAVoicemailCode>0</csm:EUAVoicemailCode>
 <csm:EUAVoicemailEmail>0</csm:EUAVoicemailEmail>
 <csm:EUAVoicemailEmailMode>0</csm:EUAVoicemailEmailMode>
 <csm:EUAMobilityTwinning>0</csm:EUAMobilityTwinning>
 <csm:EUAUnTwinningMobileNumber>0</csm:EUAUnTwinningMobileNumber>
 <csm:EUALoginCode>0</csm:EUALoginCode>
 <csm:EUARejectAutoIntercomCalls>0</csm:EUARejectAutoIntercomCalls>
 <csm:EUAPersonalDirectory>0</csm:EUAPersonalDirectory>
 <csm:EUAShortCodes>0</csm:EUAShortCodes>
 <csm:EUABlockForwarding>0</csm:EUABlockForwarding>
 <csm:EUAForwardNumber>0</csm:EUAForwardNumber>
 <csm:EUAForwardBusyNumber>0</csm:EUAForwardBusyNumber>
 <csm:EUAForwardOnBusy>0</csm:EUAForwardOnBusy>
 <csm:EUAForwardOnNoAnswer>0</csm:EUAForwardOnNoAnswer>
 <csm:EUAADSSKeys>0</csm:EUAADSSKeys>
 <csm:EUAVoicemailRingback>0</csm:EUAVoicemailRingback>
 <csm:EUAConferencePIN>0</csm:EUAConferencePIN>
 </csm:EUAAuth>
 <csm:UserRightsView />
 <csm:UsingView>false</csm:UsingView>
 <csm:UserRightsTimeProfile />
 <csm:OutOfHoursUserRights />
 <csm:Name>test09</csm:Name>
 <csm:KName />
 <csm>Password>test09</csm>Password>
 <csm:FullName />
 <csm:Extension>207</csm:Extension>
 <csm:Priority>1</csm:Priority>
 <csm:OutsideCallSeq>0</csm:OutsideCallSeq>
 <csm:InsideCallSeq>0</csm:InsideCallSeq>
 <csm:RingbackCallSeq>0</csm:RingbackCallSeq>
 <csm:NoAnswerTime>15</csm:NoAnswerTime>
 <csm:ForwardOnBusy>false</csm:ForwardOnBusy>
 <csm:BookConferenceWithPM>false</csm:BookConferenceWithPM>
 <csm:DisableForwardOnInt>false</csm:DisableForwardOnInt>
 <csm:DisableForwardUncondOnInt>false</csm:DisableForwardUncondOnInt>
 <csm:DisableForwardBusyNoAnsOnInt>false</
csm:DisableForwardBusyNoAnsOnInt>
 <csm:VoicemailReception2 />

```

```

 <csm:VoicemailReception3 />
 <csm:DSSKeys>
 <csm:DSSKey Key="1">
 <csm:KeyType>0</csm:KeyType>
 <csm:Label />
 <csm:ActionObject>39</csm:ActionObject>
 <csm:Data>a=</csm:Data>
 <csm:RingDelay>0</csm:RingDelay>
 <csm:IdlePos />
 </csm:DSSKey>
 <csm:DSSKey Key="2">
 <csm:KeyType>0</csm:KeyType>
 <csm:Label />
 <csm:ActionObject>39</csm:ActionObject>
 <csm:Data>=</csm:Data>
 <csm:RingDelay>0</csm:RingDelay>
 <csm:IdlePos />
 </csm:DSSKey>
 <csm:DSSKey Key="3">
 <csm:KeyType>0</csm:KeyType>
 <csm:Label />
 <csm:ActionObject>39</csm:ActionObject>
 <csm:Data>c=</csm:Data>
 <csm:RingDelay>0</csm:RingDelay>
 <csm:IdlePos />
 </csm:DSSKey>
 </csm:DSSKeys>
 <csm:InhibitOffSwitchForwarding>>false</csm:InhibitOffSwitchForwarding>
 <csm:IsNoUser>>false</csm:IsNoUser>
 <csm:IsRealUser>>true</csm:IsRealUser>
 <csm:IsRemoteManager>>false</csm:IsRemoteManager>
 <csm:IsVoiceEmailModeAlert>>false</csm:IsVoiceEmailModeAlert>
 <csm:IsVoiceEmailModeCopy>>false</csm:IsVoiceEmailModeCopy>
 <csm:IsVoiceEmailModeForward>>false</csm:IsVoiceEmailModeForward>
 <csm:IsVoiceEmailModeOff>>true</csm:IsVoiceEmailModeOff>
 <csm:MaxTwinnedCalls>1</csm:MaxTwinnedCalls>
 <csm:PhoneManagerCallStatusOptions>4294967295</
csm:PhoneManagerCallStatusOptions>
 <csm:PhoneManagerCloseOptions>0</csm:PhoneManagerCloseOptions>
 <csm:PhoneManagerCanChange>>true</csm:PhoneManagerCanChange>
 <csm:PhoneManagerConfigureOptions>81664</
csm:PhoneManagerConfigureOptions>
 <csm:PhoneManagerOptions>98120</csm:PhoneManagerOptions>
 <csm:PhoneManagerOptionsOriginal>98120</csm:PhoneManagerOptionsOriginal>
 <csm:PhoneType>47</csm:PhoneType>
 <csm:PhoneTypeIndex>47</csm:PhoneTypeIndex>
 <csm:PopupAnswering>>false</csm:PopupAnswering>
 <csm:PopupExternal>>false</csm:PopupExternal>
 <csm:PopupInternal>>false</csm:PopupInternal>
 <csm:PopupOutlook>>false</csm:PopupOutlook>
 <csm:PopupRingin>>false</csm:PopupRingin>
 <csm:PopupOptions>0</csm:PopupOptions>
 <csm:RingDelay>0</csm:RingDelay>
 <csm:ShowAccountCodes>>true</csm:ShowAccountCodes>
 <csm:ShowAllCalls>>true</csm:ShowAllCalls>
 <csm:ShowCallStatus>>true</csm:ShowCallStatus>
 <csm:ShowCostOfCall>>true</csm:ShowCostOfCall>
 <csm:ShowIncoming>>true</csm:ShowIncoming>
 <csm:ShowMessages>>true</csm:ShowMessages>
 <csm:ShowMissed>>true</csm:ShowMissed>
 <csm:ShowOutgoing>>true</csm:ShowOutgoing>
 <csm:ShowSpeedDials>>true</csm:ShowSpeedDials>
 <csm:StartInCompactMode>>false</csm:StartInCompactMode>
 <csm:StayInCompactModeOnIncomingCall>>false</
csm:StayInCompactModeOnIncomingCall>

```



```

 <csm:StayInCompaceModeOnOutgoingCall>false</
csm:StayInCompaceModeOnOutgoingCall>
 <csm:T3AllowThirdPartyFwd>false</csm:T3AllowThirdPartyFwd>
 <csm:T3ProtectFromThirdPartyFwd>false</csm:T3ProtectFromThirdPartyFwd>
 <csm:TwinnedDialDelay>2</csm:TwinnedDialDelay>
 <csm:TwinnedEligibleForForwarded>false</csm:TwinnedEligibleForForwarded>
 <csm:TwinnedEligibleForGroup>false</csm:TwinnedEligibleForGroup>
 <csm:TwinnedMobileNumber />
 <csm:TwinnedTimeProfile />
 <csm:TwinningNumber />
 <csm:TwinningType>0</csm:TwinningType>
 <csm:TwinningUser />
 <csm:IsTwinSlave>false</csm:IsTwinSlave>
 <csm:IsTwinMaster>false</csm:IsTwinMaster>
 <csm:InternalTwinning>false</csm:InternalTwinning>
 <csm:MobilityTwinning>false</csm:MobilityTwinning>
 <csm:TwinnedMobileAnswerGuard>0</csm:TwinnedMobileAnswerGuard>
 <csm:AutoRecMailBox>207 test21</csm:AutoRecMailBox>
 <csm:ManualRecMailBox>207 test21</csm:ManualRecMailBox>
 <csm:PA ServicesEnabled>false</csm:PA ServicesEnabled>
 <csm:AutoRecModeIn>2</csm:AutoRecModeIn>
 <csm:AutoRecModeOut>2</csm:AutoRecModeOut>
 <csm:DenyAutoIntercomCalls>false</csm:DenyAutoIntercomCalls>
 <csm:MobileCallControl>false</csm:MobileCallControl>
 <csm:SpecificBstType>47</csm:SpecificBstType>
 <csm:ForwardOnNoAnswer>false</csm:ForwardOnNoAnswer>
 <csm:ForwardUnconditional>false</csm:ForwardUnconditional>
 <csm:ForwardHuntGroupCalls>false</csm:ForwardHuntGroupCalls>
 <csm:ForwardNumber />
 <csm:ForwardBusyNumber />
 <csm:DoNotDisturb>false</csm:DoNotDisturb>
 <csm:DNDEExceptions />
 <csm:OutgoingCallBar>false</csm:OutgoingCallBar>
 <csm:IncomingCallBar>false</csm:IncomingCallBar>
 <csm:OffHookStation>false</csm:OffHookStation>
 <csm:BusyOnHeld>false</csm:BusyOnHeld>
 <csm:FollowMeNumber />
 <csm:CallWaitingOn>false</csm:CallWaitingOn>
 <csm:VoicemailOn>true</csm:VoicemailOn>
 <csm:VoicemailHelp>false</csm:VoicemailHelp>
 <csm:VoicemailCode />
 <csm:VoicemailEmail />
 <csm:VoicemailEmailReading>false</csm:VoicemailEmailReading>
 <csm:VoicemailReception />
 <csm:VoicemailEmailMode>0</csm:VoicemailEmailMode>
 <csm:VoicemailRingback>false</csm:VoicemailRingback>
 <csm:ShortCodes>
 <csm:ShortCode>
 <csm:Code>*DSS1</csm:Code>
 <csm:TelephoneNumber>99/a=</csm:TelephoneNumber>
 <csm:LineGroupId>0</csm:LineGroupId>
 <csm:Feature>26</csm:Feature>
 <csm:Locale />
 <csm:ForceAccountCode>false</csm:ForceAccountCode>
 <csm:ForceAuthCode>false</csm:ForceAuthCode>
 </csm:ShortCode>
 <csm:ShortCode>
 <csm:Code>*DSS2</csm:Code>
 <csm:TelephoneNumber>99/b=</csm:TelephoneNumber>
 <csm:LineGroupId>0</csm:LineGroupId>
 <csm:Feature>26</csm:Feature>
 <csm:Locale />
 <csm:ForceAccountCode>false</csm:ForceAccountCode>
 <csm:ForceAuthCode>false</csm:ForceAuthCode>
 </csm:ShortCode>
 </csm:ShortCodes>

```

```

 <csm:ShortCode>
 <csm:Code>*DSS3</csm:Code>
 <csm:TelephoneNumber>99/c=</csm:TelephoneNumber>
 <csm:LineGroupId>0</csm:LineGroupId>
 <csm:Feature>26</csm:Feature>
 <csm:Locale />
 <csm:ForceAccountCode>>false</csm:ForceAccountCode>
 <csm:ForceAuthCode>>false</csm:ForceAuthCode>
 </csm:ShortCode>
 </csm:ShortCodes>
 <csm:DialInOn>>false</csm:DialInOn>
 <csm:DialInTimeProfile />
 <csm:DialInFirewallProfile />
 <csm:SourceNumbers>V207|</csm:SourceNumbers>
 <csm:DialInQuotaTime>0</csm:DialInQuotaTime>
 <csm:LoginCode />
 <csm>LoginIdleTime />
 <csm:WrapUpTime>2</csm:WrapUpTime>
 <csm:TwinMaster />
 <csm:SecTwinCallEnabled>>false</csm:SecTwinCallEnabled>
 <csm:CanIntrude>>false</csm:CanIntrude>
 <csm:CannotBeIntruded>>true</csm:CannotBeIntruded>
 <csm:XDirectory>>false</csm:XDirectory>
 <csm:ForceLogin>>false</csm:ForceLogin>
 <csm:ForceAuthCode>>false</csm:ForceAuthCode>
 <csm:ForceAccountCode>>false</csm:ForceAccountCode>
 <csm:SystemPhone>0</csm:SystemPhone>
 <csm:AbsentMsg>0</csm:AbsentMsg>
 <csm:AbsentSet>0</csm:AbsentSet>
 <csm:AbsentText />
 <csm:T3HuntGroupMembershipStatus />
 <csm:T3HuntGroupServiceStatus />
 <csm:T3HuntGroupNightServiceStatus />
 <csm:T3DirectoryEntries />
 <csm:MonitorGroup />
 <csm:DisplayLocale> </csm:DisplayLocale>
 <csm:Locale />
 <csm:PMTType>0</csm:PMTType>
 <csm:InboundAutoRecord>0</csm:InboundAutoRecord>
 <csm:OutboundAutoRecord>0</csm:OutboundAutoRecord>
 <csm:AutoRecordTimeProfile />
 <csm:RemoteWorker>>false</csm:RemoteWorker>
 <csm:CanAcceptCollectCalls>>false</csm:CanAcceptCollectCalls>
 <csm>UserRights />
 <csm:Secretaries />
 <csm:TransferReturnTime />
 <csm:AnswerCallWaiting>>true</csm:AnswerCallWaiting>
 <csm:RingingLinePreference>>true</csm:RingingLinePreference>
 <csm:IdleLinePreference>>true</csm:IdleLinePreference>
 <csm:CoverageTime>10</csm:CoverageTime>
 <csm:AutoVRL>0</csm:AutoVRL>
 <csm:ManualVRL>0</csm:ManualVRL>
 <csm:DelayedRingPreference>>false</csm:DelayedRingPreference>
 <csm:AnswerPreSelect>>false</csm:AnswerPreSelect>
 <csm:ReserveLastCA>>false</csm:ReserveLastCA>
 <csm:CallTracingOn>>false</csm:CallTracingOn>
 <csm:DisplayCharges>>true</csm:DisplayCharges>
 <csm:MarkUpFactor>100</csm:MarkUpFactor>
 <csm:reset_longest_idle_info>0</csm:reset_longest_idle_info>
 <csm:NoAnswerStatus>0</csm:NoAnswerStatus>
 <csm:PBXAddress />
 <csm:SIPName>207</csm:SIPName>
 <csm:SIPDisplayName>test21</csm:SIPDisplayName>
 <csm:SIPContact>207</csm:SIPContact>
 <csm:SIPAnonymous>>false</csm:SIPAnonymous>

```



```

<csm:AbbreviatedRing>true</csm:AbbreviatedRing>
<csm:CustomerServiceRep>>false</csm:CustomerServiceRep>
<csm:ACWTime>-1</csm:ACWTime>
<csm:AutoACW>>false</csm:AutoACW>
<csm:UMSWebServices>>false</csm:UMSWebServices>
<csm:DisableVMOnFU>>false</csm:DisableVMOnFU>
<csm:DTMFCallCtrl>>false</csm:DTMFCallCtrl>
<csm:LoggedOutTwinning>0</csm:LoggedOutTwinning>
<csm:OneXClient>>false</csm:OneXClient>
<csm:MobilityFeatures>>false</csm:MobilityFeatures>
<csm:TwinnedBridgeAppearances>>false</csm:TwinnedBridgeAppearances>
<csm:TwinnedCoverageAppearances>>false</csm:TwinnedCoverageAppearances>
<csm:TwinnedLineAppearances>>false</csm:TwinnedLineAppearances>
<csm:PersonalDirectory />
<csm:ForwardToVoicemail>>false</csm:ForwardToVoicemail>
<csm:CoverageGroup />
<csm:CanChangeHGOOSGroup />
<csm:CanChangeHGONGroup />
<csm:IncludeForwardInMenu>>true</csm:IncludeForwardInMenu>
<csm:CallLoggingCentralised>0</csm:CallLoggingCentralised>
<csm:AttentionRing>true</csm:AttentionRing>
<csm:CoverageRing>0</csm:CoverageRing>
<csm:LogMissedCallsForHG />
<csm:DisableForwardToVoicemail>0</csm:DisableForwardToVoicemail>
<csm:AnnouncementsOn>>false</csm:AnnouncementsOn>
<csm:FollowAnnouncementsOn>true</csm:FollowAnnouncementsOn>
<csm:LoopAnnouncementsOn>true</csm:LoopAnnouncementsOn>
<csm:SyncAnnouncementsOn>>false</csm:SyncAnnouncementsOn>
<csm:FirstAnnTime>10</csm:FirstAnnTime>
<csm:SecondAnnTime>20</csm:SecondAnnTime>
<csm:BetweenAnnTime>20</csm:BetweenAnnTime>
<csm:PostAnnTone>2</csm:PostAnnTone>
<csm:PortalServices>0</csm:PortalServices>
<csm:WorkingHoursUserRightsGroup />
<csm:T3SelfAdmin>>false</csm:T3SelfAdmin>
<csm:MobileCallback>>false</csm:MobileCallback>
<csm:Receptionist>true</csm:Receptionist>
<csm:SoftPhone>>false</csm:SoftPhone>
<csm:OneXTelecommuter>>false</csm:OneXTelecommuter>
<csm:AssignedPackage>1</csm:AssignedPackage>
<csm:AutoRecMode>2</csm:AutoRecMode>
<csm:CallLogTimeout>00:00</csm:CallLogTimeout>
<csm:UserCLI />
<csm:FlareEnabled>>false</csm:FlareEnabled>
<csm:FlareMode>0</csm:FlareMode>
<csm:AutoIntDeny>>false</csm:AutoIntDeny>
<csm:TUIUser>
 <csm:TUIFeaturesMenuControls>>false</csm:TUIFeaturesMenuControls>
 <csm:TUIFeaturesMenu>true</csm:TUIFeaturesMenu>
 <csm:TUIBasicCallFunctions>true</csm:TUIBasicCallFunctions>
 <csm:TUIAdvancedCallFunctions>true</csm:TUIAdvancedCallFunctions>
 <csm:TUIHotDeskFunctions>true</csm:TUIHotDeskFunctions>
 <csm:TUIPasscodeChange>true</csm:TUIPasscodeChange>
 <csm:TUIPhoneLock>true</csm:TUIPhoneLock>
 <csm:TUISelfAdmin>true</csm:TUISelfAdmin>
 <csm:TUIVoiceMailControls>true</csm:TUIVoiceMailControls>
 <csm:TUIForwarding>true</csm:TUIForwarding>
</csm:TUIUser>
<csm>UserPasswordStatus>1</csm>UserPasswordStatus>
<csm:BlockForwarding>>false</csm:BlockForwarding>
<csm:ParkAndPageInfo>
 <csm:ParkAndPage>
 <csm:ParkAndPageId>1</csm:ParkAndPageId>
 <csm:PagingNumber />
 <csm:CentrexTransferNumber />

```

```

 <csm:PNPFallBackNumber />
 <csm:RetryTimeout>15</csm:RetryTimeout>
 <csm:RetryCount>0</csm:RetryCount>
 </csm:ParkAndPage>
 <csm:ParkAndPage>
 <csm:ParkAndPageId>2</csm:ParkAndPageId>
 <csm:PagingNumber />
 <csm:CentrexTransferNumber />
 <csm:PNPFallBackNumber />
 <csm:RetryTimeout>15</csm:RetryTimeout>
 <csm:RetryCount>0</csm:RetryCount>
 </csm:ParkAndPage>
 <csm:ParkAndPage>
 <csm:ParkAndPageId>3</csm:ParkAndPageId>
 <csm:PagingNumber />
 <csm:CentrexTransferNumber />
 <csm:PNPFallBackNumber />
 <csm:RetryTimeout>15</csm:RetryTimeout>
 <csm:RetryCount>0</csm:RetryCount>
 </csm:ParkAndPage>
 </csm:ParkAndPageInfo>
 <csm:MobileVoIPClientEnabled>false</csm:MobileVoIPClientEnabled>
 <csm:SendMobilityEmail>false</csm:SendMobilityEmail>
 <csm:IPOCCAgent>false</csm:IPOCCAgent>
 <csm:AgentType>0</csm:AgentType>
 <csm:WebCollaboration>false</csm:WebCollaboration>
 <csm:ConferencePIN />
 </csm:User>
</csm:ws_object>
</csm:data>
</commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema for bulk import and export of Presence Profile

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:complexType name="XmlPsCommProfile">
 <xsd:complexContent>
 <xsd:extension base="one:xmlCommProfileType" >
 <xsd:sequence>
 <xsd:element name="primarySipEntityId" type="xsd:long"/>
 <xsd:element name="secondarySipEntityId" type="xsd:long" minOccurs="0"/>
 </xsd:sequence>
 </xsd:extension>
 </xsd:complexContent>
</xsd:complexType>

```

## Sample XML for Presence Communication Profile

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd ">
 <tns:user>
 <authenticationType>BASIC</authenticationType>
 <description>description</description>
 <displayName>pm_0displayName</displayName>
 <displayNameAscii>pm_0displayNameAscii</displayNameAscii>
 <dn>dn</dn>
 <isDuplicatedLoginAllowed>true</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>pm_0givenName</givenName>
 </tns:user>
</tns:users>

```

```

<honorific>honorific</honorific>
<loginName>pm_0@pres.avaya.com</loginName>
<middleName>pm_0middleName</middleName>
<managerName>pm_0managerName</managerName>
<preferredGivenName>pm_0preferredGivenName</preferredGivenName>
<preferredLanguage>en-US</preferredLanguage>
<source>local</source>
<sourceUserKey>sourceUserKey</sourceUserKey>
<status>AUTHPENDING</status>
<suffix>suffix</suffix>
<surname>pm_0surname</surname>
<title>pm_0title</title>
<userName>pm_0userName</userName>
<userPassword>-6396392681329505585</userPassword>
<commPassword>-6396392681329505585</commPassword>
<userType>AGENT</userType>
<address>
<addressType>OFFICE</addressType>
<name>pm_0contact_address</name>
<building>pm_0building</building>
<localityName>pm_0localityName</localityName>
<postalCode>pm_0postalCode</postalCode>
<room>pm_0room</room>
<stateOrProvince>pm_0stateOrProvince</stateOrProvince>
<country>pm_0country</country>
<street>pm_0street</street>
<postalAddress>pm_0postalAddress</postalAddress>
<isPrivate>true</isPrivate>
</address>
<securityIdentity>
<identity>pm_0identity1</identity>
<realm>pm_0realm1</realm>
<type>pm_0type1</type>
</securityIdentity>
<ownedContactLists>
<contactList>
<name>pm_0ContactList_1</name>
<description>pm_0Description_ContactList_default_1</description>
<isPublic>false</isPublic>
<members>
<memberContact>pm_0_0Contact_1</memberContact>
<speedDialContactAddress>
<address>12345</address>
<altLabel>pm_0altLabel1</altLabel>
<contactCategory>OFFICE</contactCategory>
<contactType>PHONE</contactType>
<label>pm_0labe2</label>
</speedDialContactAddress>
<isFavorite>true</isFavorite>
<isSpeedDial>true</isSpeedDial>
<speedDialEntry>22222</speedDialEntry>
<isPresenceBuddy>true</isPresenceBuddy>
<label>pm_0labe3</label>
<altLabel>pm_0altLabe4</altLabel>
<description>pm_0description1</description>
<priorityLevel>1</priorityLevel>
</members>
<contactListType>CONTACTCENTER</contactListType>
</contactList>
</ownedContactLists>
<ownedContacts>
<contact>
<company>pm_0company1</company>
<description>pm_0description1</description>
<displayName>pm_0_0Contact_1</displayName>

```

```

<displayNameAscii>pm_0displayNameAscii1</displayNameAscii>
<dn>pm_0dn1</dn>
<givenName>pm_0givenName1</givenName>
<initials>initials1</initials>
<middleName>pm_0middleName1</middleName>
<preferredGivenName>pm_0preferredGivenName1</preferredGivenName>
<preferredLanguage>English</preferredLanguage>
<isPublic>false</isPublic>
<source>local</source>
<sourceUserKey>pm_0sourceUserKey1</sourceUserKey>
<suffix>pm_0suffix1</suffix>
<surname>pm_0surname1</surname>
<title>pm_0title1</title>
<ContactAddress>
<address>12345</address>
<altLabel>pm_0altLabel1</altLabel>
<contactCategory>OFFICE</contactCategory>
<contactType>PHONE</contactType>
<label>pm_0label1</label>
</ContactAddress>
<addresses>
<addressType>OFFICE</addressType>
<name>pm_0_Add_Name</name>
<building>pm_0_Building_Name</building>
<localityName>pm_0_locality</localityName>
<postalCode>411014</postalCode>
<room>pm_0_Room_5B</room>
<stateOrProvince>Maharashtr<A/stateOrProvince>
<country>Indi<A/country>
<street>pm_0_Street</street>
<postalAddress>pm_0_POAdd</postalAddress>
<isPrivate>true</isPrivate>
</addresses>
</contact>
</ownedContacts>
<presenceUserDefault>
<infoTypeAccess>
<infoType>
<label>All</label>
<filter>ALL</filter>
<specFlags>FULL</specFlags>
</infoType>
<access>BLOCK</access>
</infoTypeAccess>
</presenceUserDefault>
<presenceUserACL>
<infoTypeAccess>
<infoType>
<label>All</label>
<filter>ALL</filter>
<specFlags>FULL</specFlags>
</infoType>
<access>BLOCK</access>
</infoTypeAccess>
<watcherDisplayName>pm_0_0Contact_1</watcherDisplayName>
</presenceUserACL>
<presenceUserCLDefault>
<infoTypeAccess>
<infoType>
<label>Telephony</label>
<filter>CLASS (phone)</filter>
<specFlags></specFlags>
</infoType>
<access>ALLOW</access>
</infoTypeAccess>

```

```

</presenceUserCLDefault>
<commProfileSet>
<commProfileSetName>commProfileSetNamepm_0</commProfileSetName>
<isPrimary>true</isPrimary>
<handleList>
<handle>
<handleName>smtp_pm_0@ahmadexserver.com</handleName>
<handleType>smtp</handleType>
<handleSubType>msexchange</handleSubType>
<domainName>__foreign__</domainName>
</handle>
</handleList>
<commProfileList>
<commProfile xsi:type="ext:XmlPsCommProfile"
xmlns:ext="http://xml.avaya.com/schema/presence">
<commProfileType>PS</commProfileType>
<ext:primarySipEntityId>32768</ext:primarySipEntityId>
</commProfile>
</commProfileList>
</commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema for Conferencing Communication Profile

```

<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:one="http://xml.avaya.com/schema/import"
targetNamespace="http://xml.avaya.com/schema/import_mmcs"
elementFormDefault="qualified"
xmlns:abc="http://xml.avaya.com/schema/import_mmcs">
<xsd:import namespace="http://xml.avaya.com/schema/import"
schemaLocation="userimport.xsd"/>
<xsd:complexType name="MmcsCommProfileType">
<xsd:complexContent>
<xsd:extension base="one:xmlCommProfileType" >
<xsd:sequence>
<xsd:element name="template" type="xsd:string"/>
<xsd:element name="securityCode" type="xsd:string"/>
<xsd:element name="moderatorPin" type="xsd:string"/>
<xsd:element name="participantPasscode" type="xsd:string"/>
<xsd:element name="moderatorPasscode" type="xsd:string"/>
<xsd:element name="eventConfCode" type="xsd:string"/>
<xsd:element name="location" type="xsd:string" minOccurs="0"/>
<xsd:element name="autoGeneratedCodeLength" minOccurs="0">
<xsd:simpleType>
<xsd:restriction base="xsd:int">
<xsd:minInclusive value="6"/>
<xsd:maxInclusive value="8"/>
</xsd:restriction>
</xsd:simpleType>
</xsd:element>
</xsd:sequence>
</xsd:extension>
</xsd:complexContent>
</xsd:complexType>
</xsd:schema>

```

## Sample XML for bulk import of Conferencing Profile

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:users xmlns:tns="http://xml.avaya.com/schema/import"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">

<!-- User Record for: 55555555@domain.com -->

```

```

 <tns:user>

 (Other user elements are required here - consult the main user record XML schema
 reference)

 <!-- Here, a Communication Profile is defined for the user -->
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>

 <!-- The user must be given one or more handles (of type "SIP" or E.164) -->
 <handleList>
 <handle>
 <handleName>5555555</handleName>
 <handleType>sip</handleType>
 <handleSubType>username</handleSubType>
 <domainName>domain.com</domainName>
 </handle>
 </handleList>

 <!-- Here, one or more product-specific profiles may be Defined -->
 <commProfileList>
 <commProfile xsi:type="ns2:MmcsCommProfileType" xmlns:ns2="http://
xml.avaya.com/schema/import_mmcs">
 <commProfileType>mmcsCommProfile</commProfileType>
 <ns2:template>event_1000</ns2:template>
 <ns2:securityCode></ns2:securityCode>
 <ns2:moderatorPin></ns2:moderatorPin>
 <ns2:participantPasscode></ns2:participantPasscode>
 <ns2:moderatorPasscode></ns2:moderatorPasscode>
 <ns2:eventConfCode>777</ns2:eventConfCode>
 <ns2:location>Location1</ns2:location>
 <ns2:autoGeneratedCodeLength>6</ns2:autoGeneratedCodeLength>
 </commProfile>
 </commProfileList>
 </commProfileSet>
</tns:user>
</tns:users>

```

## XML Schema Definition for bulk import of global setting records

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/import" xmlns:ext="http://
xml.avaya.com/schema/import" xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.avaya.com/schema/import" version="1.0">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 This Schema defines schema for bulk import and export of System ACL, Public
 Contacts and Shared Address.
 </xs:documentation>
 </xs:annotation>
 <xs:element name="presenceSystemDefault" type="tns:xmlPresSystemDefaultType"/>
 <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType"/>
 <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"/>
 <xs:element name="presenceSystemACL" type="tns:xmlPresSystemACLEntryType"/>
 <xs:element name="publicContact" type="tns:xmlPublicContact"/>
 <xs:element name="globalSettings" type="tns:globalSettingsType"/>
 <xs:element name="sharedAddress" type="tns:xmlSharedAddress"/>
 <xs:complexType name="globalSettingsType">
 <xs:annotation>
 <xs:documentation xml:lang="en">

```

```

---Root Element 'presenceSystemDefault' represent a global default that
 defines access to presence if none of the more specific rules apply.
 There must be at least one System Default rule defined.
---Root Element 'presenceEnforcedUserACL' represent collection of
 Enforced User ACL (containing 1 or more Enforced User ACL).This rule
 is similar to a User ACL in the sense that its entries define access
 between individual presentities and watchers. However this rule is
 managed by the administrator as opposed to presentities themselves.
 Entries of Enforced User ACL can also be defined with different
 priorities. Entries with higher priority will have more weight than
 entries with lower priority.
---Root Element 'presenceSystemRule' represent collection of System
 Rules (containing 1 or more System Rules).Global rules that enforce
 certain level of presence access for everyone in the solution. There
 may be several rules that apply to all presentities and all watchers.
 System Rules are used to enforce global policies. For example, a
 system rule can declare that telephony presence should be available
 to everybody in the company. System Rules can be defined with
 different priorities. Rules with higher priority will have more
 weight than rules with lower priority
---Root Element 'presenceSystemACL' represent collection of System ACL
 (containing 1 or more System ACL).
 System ACL (Access Control List) - are enterprise-wide rules that can
 allow a watcher to see presence of all users or deny a watcher from
 accessing anyone's presence. There may be several entries in the
 list, each entry corresponding to one watcher. System ACL is
 normally used to provide critical system services with a privileged
 access to presence of all users.
---Root Element 'publicContact' represent collection of public contacts
 (containing 1 or more public contacts).A personal contact is owned
 by an individual user and is not accessible to all users. A public
 contact can be shared by all users and is owned by the default
 system user.
---Root Element 'sharedAddress' represent collection of shared Address
 (containing 1 or more shared Addresses).A shared Address can be
 shared by all users.
 </xs:documentation>
 </xs:annotation>
 <xs:sequence>
 <xs:element name="presenceSystemDefault"
type="tns:xmlPresSystemDefaultType" minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="presenceEnforcedUserACL"
type="tns:xmlPresEnforcedUserACLEntryType" minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="presenceSystemRule" type="tns:xmlPresSystemRuleType"
minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="presenceSystemACL" type="tns:xmlPresSystemACLEntryType"
minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="sharedAddress" type="tns:xmlSharedAddress" minOccurs="0"
maxOccurs="unbounded"/>
 <xs:element name="publicContact" type="tns:xmlPublicContact" minOccurs="0"
maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlSharedAddress">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ---addressType:The unique text name of the address type.
 Possible values are: Home, business.
 ---name: The Name property defines the unique label by which
 the address is known. Default format for user specific
 address should include user name place address type.
 ---building:The name or other designation of a structure.
 ---localityName:The name of a locality, such as a city, county
 or other geographic region.
 </xs:documentation>
 </xs:annotation>
 </xs:sequence>
</xs:complexType>

```



```

 ---postalCode:A code used by postal services to route mail to a
 destination. In the United States this is the zip code.
 ---room:Name or designation of a room.
 ---stateOrProvince:The full name of a state or province.
 ---country:A country.
 ---street:The physical address of the object such as an address
 for package delivery
 ---postalAddress:A free formed text area for the complete
 physical delivery address. It may be used in place of the
 specific fields in this table.
 ---readOnly:A boolean indicator showing whether or not the
 address can be changed from its default value.
 </xs:documentation>
</xs:annotation>
<xs:element name="addressType" type="xs:string"/>
<xs:element name="name" type="xs:string"/>
<xs:element name="building" type="xs:string" minOccurs="0"/>
<xs:element name="localityName" type="xs:string" minOccurs="0"/>
<xs:element name="postalCode" type="xs:string" minOccurs="0"/>
<xs:element name="room" type="xs:string" minOccurs="0"/>
<xs:element name="stateOrProvince" type="xs:string" minOccurs="0"/>
<xs:element name="country" type="xs:string" minOccurs="0"/>
<xs:element name="street" type="xs:string" minOccurs="0"/>
<xs:element name="postalAddress" minOccurs="0">
 <xs:simpleType>
 <xs:restriction base="xs:string">
 <xs:maxLength value="1024"/>
 </xs:restriction>
 </xs:simpleType>
</xs:element>
<xs:element name="readOnly" type="xs:boolean" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPublicContact">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ---company:The organization that the contact belongs to.
 ---description: A free text field containing human readable
 text providing information on this entry.
 ---displayName:The localized name of a contact to be used when
 displaying. It will typically be the localized full name.
 This value may be provisioned from the user's enterprise
 directory entry. If it does not exist, synchronization
 rules can be used to populate it for other fields
 e.g. Surname, GivenName, or LoginName.
 ---displayNameAscii:The full text name of the contact
 represented in ASCII. It is used to support display
 (e.g. endpoints) that cannot handle localized text.
 ---dn:The distinguished name of the user. The DN is a sequence
 of relative distinguished names (RDN) connected by commas.
 An RDN is an attribute with an associated value in the form
 of attribute=value, normally expressed in a UTF-8 string
 format. The dn can be used to uniquely identify this
 record. Note the dn is changeable.
 ---givenName:The first name of the contact.
 ---initials:Initials of the contact.
 ---middleName:The middle name of the contact.
 ---preferredGivenName:The nick name of the contact.
 ---preferredLanguage:The individual's preferred written or
 spoken language. Values will conform to rfc4646 and the
 reader should refer to rfc4646 for syntax. This format
 uses the ISO standard Language (ISO-639) and region
 (ISO-3166) codes In the absence of a value the client's
 locale should be used, if no value is set, en-US should be

```



```

 defaulted.
 ---source:Free format text field that identifies the entity
 that created this user record. The format of this field
 will be either a IP Address/Port or a name representing an
 enterprise LDAP or Avaya.
 ---sourceUserKey:The key of the user from the source system. If
 the source is an Enterprise Active Directory server, this
 value will be the objectGUID.
 ---suffix:The text appended to a name e.g. Jr., III.
 ---surname:The user's last name, also called the family name.
 ---title:The job function of a person in their organizational
 context.Examples: supervisor, manager.
 ---contactAddresses:A Entity used to store a contact's address.
 ---addresses:A fully qualified URI for interacting with this
 contact. Any addresses added to this entity should contain
 a qualifier e.g. sip, sips, tel, mailto. The address should
 be syntactically valid based on the qualifier. It must be
 possible to add via the GUI and Interface. The application
 must do validation.
 </xs:documentation>
</xs:annotation>
<xs:element name="company" type="xs:string" minOccurs="0"/>
<xs:element name="description" type="xs:string" minOccurs="0"/>
<xs:element name="displayName" type="xs:string"/>
<xs:element name="displayNameAscii" type="xs:string"/>
<xs:element name="dn" type="xs:string" minOccurs="0"/>
<xs:element name="givenName" type="xs:string"/>
<xs:element name="initials" type="xs:string" minOccurs="0"/>
<xs:element name="middleName" type="xs:string" minOccurs="0"/>
<xs:element name="preferredGivenName" type="xs:string" minOccurs="0"/>
<xs:element name="preferredLanguage" type="xs:string" minOccurs="0"/>
<xs:element name="source" type="xs:string"/>
<xs:element name="sourceUserKey" type="xs:string"/>
<xs:element name="suffix" type="xs:string" minOccurs="0"/>
<xs:element name="surname" type="xs:string"/>
<xs:element name="title" type="xs:string" minOccurs="0"/>
<xs:element name="contactAddresses" type="tns:xmlContactAddressList"
minOccurs="0"/>
 <xs:element name="addresses" type="tns:xmlAddressList" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContactAddressList">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ContactAddressList: A list containing Contact Addresses
 </xs:documentation>
 </xs:annotation>
 <xs:sequence>
 <xs:element name="contact" type="tns:xmlContactAddress" minOccurs="0"
maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlContactAddress">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ---type:The value reflecting the type of handle this is.
 Possible values are "username","e164", and
 "privatesubsystem"
 ---category:The value representing a further qualification to
 the contact address.
 Possible values include Office, Home, Mobile.
 ---handle:This is the name given to the user to allow
 communication to be established with the user. It is an
 alphanumeric value that must comply with the userinfo
 </xs:documentation>
 </xs:annotation>
 </xs:sequence>

```

```

 related portion of a URI as described in rfc2396. However,
 it is further restricted as ASCII characters with only the
 "+" prefix to signify this is an E.164 handle and "-" and
 "." special characters supported. The handle and type together
 are unique within a specific domain. Note, the handle plus
 domain can be used to construct a user's Address of Record.
 ---label:A free text description for classifying this contact.
 ---altLabel:A free text description for classifying this
 contact. This is similar to ContactLabel, but it is used to
 store alternate language representations.
 </xs:documentation>
</xs:annotation>
<xs:element name="type" type="xs:string"/>
<xs:element name="category" type="xs:string" minOccurs="0"/>
<xs:element name="handle" type="xs:string"/>
<xs:element name="label" type="xs:string" minOccurs="0"/>
<xs:element name="altLabel" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<xs:complexType name="xmlAddressList">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 AddressList: A list containing Addresses
 </xs:documentation>
 </xs:annotation>
 <xs:sequence>
 <xs:element name="address" type="tns:xmlAddress" minOccurs="0"
maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlAddress">
 <xs:complexContent>
 <xs:extension base="tns:xmlSharedAddress">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 private:A boolean indicator to specify if this
 attribute set could be shared across multiple
 users. Private attributes sets can only be owned
 by a single user. Default=false.
 </xs:documentation>
 </xs:annotation>
 <xs:element name="private" type="xs:boolean"/>
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresInfoTypeAccessType">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ---accessLevel:possible values:IM,Telephony
 ---action:Action possible values: ALLOW, BLOCK, CONFIRM,
 PENDING, UNDEFINED
 </xs:documentation>
 </xs:annotation>
 <xs:element name="accessLevel" type="xs:string"/>
 <xs:element name="action" type="xs:string"/>
 </xs:sequence>
</xs:complexType>
<xs:complexType name="xmlPresACRuleType">
 <xs:sequence>
 <xs:element name="infoTypeAccess" type="tns:xmlPresInfoTypeAccessType"
minOccurs="0" maxOccurs="unbounded"/>
 </xs:sequence>

```

```

</xs:complexType>
<xs:complexType name="xmlPresSystemDefaultType">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 'presenceSystemDefault' represent a global default that defines
 access to presence if none of the more specific rules apply.
 There must be at least one System Default rule defined.
 </xs:documentation>
 </xs:annotation>
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType"/>
 </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresSystemRuleType">
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 'presenceSystemRule' represent collection of System
 Rules (containing 1 or more System Rules).Global rules
 that enforce certain level of presence access for
 everyone in the solution. There may be several rules
 that apply to all presentities and all watchers.
 System Rules are used to enforce global policies.
 For example, a system rule can declare that telephony
 presence should be available to everybody in the
 company. System Rules can be defined with different
 priorities.
 Rules with higher priority will have more weight than
 rules with lower priority apply to all presentities and
 all watchers.
 ---priority:Entries of Enforced User ACL can also be
 defined with different priorities. Entries with higher
 priority will have more weight than entries with lower
 priority.
 </xs:documentation>
 </xs:annotation>
 <xs:element name="priority" type="xs:string"/>
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresSystemACLEntryType">
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ---'presenceSystemACL' represent collection of System ACL
 (containing 1 or more System ACL).System ACL
 (Access Control List) - are enterprise-wide rules that
 can allow a watcher to see presence of all users or
 deny a watcher from accessing anyone's presence. There
 may be several entries in the list, each entry
 corresponding to one watcher. System ACL is normally
 used to provide critical system services with a
 privileged access to presence of all users.
 ---watcherLoginName:LoginName of the watcher. This value
 needs to be specified if watcher is a user.
 ---watcherDisplayName:DisplayName of the watcher. This
 value needs to be specified if watcher is a Contact
 </xs:documentation>
 </xs:annotation>
 <xs:choice>

```

```

minOccurs="0"/>
 <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
 <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
 </xs:choice>
 </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
<xs:complexType name="xmlPresEnforcedUserACLEntryType">
 <xs:complexContent>
 <xs:extension base="tns:xmlPresACRuleType">
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ---'presenceEnforcedUserACL' represent collection of
 Enforced User ACL (containing 1 or more Enforced
 User ACL).This rule is similar to a User ACL in the
 sense that its entries define access between
 individual presentities and watchers. However this
 rule is managed by the administrator as opposed to
 presentities themselves. Entries of Enforced User ACL
 can also be defined with different priorities. Entries
 with higher priority will have more weight than entries
 with lower priority.
 ---watcherLoginName:LoginName of the watcher. This value
 needs to be specified if watcher is a user.
 ---watcherDisplayName:DisplayName of the watcher. This
 value needs to be specified if watcher is a Contact
 ---priority:Entries of Enforced User ACL can also be
 defined with different priorities. Entries with higher
 priority will have more weight than entries with lower
 priority.
 ---userName:LoginName of the presentity.
 </xs:documentation>
 </xs:annotation>
 <xs:element name="userName" type="xs:string"/>
 <xs:choice>
 <xs:element name="watcherLoginName" type="xs:string"
minOccurs="0"/>
 <xs:element name="watcherDisplayName" type="xs:string"
minOccurs="0"/>
 </xs:choice>
 <xs:element name="priority" type="xs:string"/>
 </xs:sequence>
 </xs:extension>
 </xs:complexContent>
</xs:complexType>
</xs:schema>

```

### Sample XML for bulk import of global setting records

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:globalSettings xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/
import systemPresence.xsd ">

 <!--
 Root Element 'presenceSystemDefault' represent a global default that defines
 access to presence if none of the more specific rules apply. There must
 be at least one System Default rule defined.
 accessLevel:possible values:ALL,Telephony
 action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
 -->
 <tns:presenceSystemDefault>

```

```

 <infoTypeAccess>
 <accessLevel>ALL</accessLevel>
 <action>ALLOW</action>
 </infoTypeAccess>
 </tns:presenceSystemDefault>
<!--
 Root Element 'presenceEnforcedUserACL' represent collection of Enforced
 User ACL (containing 1 or more Enforced User ACL).This rule is
 similar to a User ACL in the sense that its entries define access
 between individual presentities and watchers. However this rule is
 managed by the administrator as opposed to presentities themselves.
 Entries of Enforced User ACL can also be defined with different
 priorities. Entries with higher priority will have more weight than
 entries with lower priority.
 ---accessLevel:possible values:ALL,Telephony
 ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
 ---watcherLoginName>LoginName of the watcher. This value needs to be
 specified if watcher is a user.
 ---watcherDisplayName>DisplayName of the watcher. This value needs to be
 specified if watcher is a Contact
 ---priority>Entries of Enforced User ACL can also be defined with different
 priorities. Entries with higher priority will have more weight than
 entries with lower priority.
 ---userName>LoginName of the presentity.
-->
 <tns:presenceEnforcedUserACL>
 <infoTypeAccess>
 <accessLevel>Telephony</accessLevel>
 <action>BLOCK</action>
 </infoTypeAccess>
 <userName>jmiller@avaya.com</userName>
 <watcherLoginName>userlogin2@avaya.com</watcherLoginName>
 <priority>HIGH</priority>
 </tns:presenceEnforcedUserACL>
<!--
 Root Element 'presenceSystemRule' represent collection of System Rules
 (containing 1 or more System Rules).Global rules that enforce certain level
 of presence access for everyone in the solution. There may be several rules
 that apply to all presentities and all watchers. System Rules are used to
 enforce global policies. For example, a system rule can declare that
 telephony presence should be available to everybody in the company.
 System Rules can be defined with different priorities. Rules with higher
 priority will have more weight than rules with lower priority
 ---accessLevel:possible values:IM,Telephony
 ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
 ---watcherLoginName>LoginName of the watcher. This value needs to be specified
 if watcher is a user.
 ---watcherDisplayName>DisplayName of the watcher. This value needs to be
 specified if watcher is a Contact
 ---priority>Entries of Enforced User ACL can also be defined with different
 priorities. Entries with higher priority will have more weight than
 entries with lower priority.
-->
 <tns:presenceSystemRule>
 <infoTypeAccess>
 <accessLevel>Telephony</accessLevel>
 <action>ALLOW</action>
 </infoTypeAccess>
 <priority>HIGH</priority>
 </tns:presenceSystemRule>
<!--
 Root Element 'presenceSystemACL' represent collection of System ACL
 (containing 1 or more System ACL).
 System ACL (Access Control List) - are enterprise-wide rules that can allow
 a watcher to see presence of all users or deny a watcher from accessing

```

```

 anyone's presence. There may be several entries in the list, each entry
 corresponding to one watcher. System ACL is normally used to provide
 critical system services with a privileged access to presence of all users.
 ---accessLevel:possible values:IM,Telephony
 ---action:Action possible values: ALLOW, BLOCK, CONFIRM, PENDING, UNDEFINED
 ---watcherLoginName>LoginName of the watcher. This value needs to be specified
 if watcher is a user.
-->
<tns:presenceSystemACL>
 <infoTypeAccess>
 <accessLevel>Telephony</accessLevel>
 <action>BLOCK</action>
 </infoTypeAccess>
 <watcherLoginName>jmiller@avaya.com</watcherLoginName>
</tns:presenceSystemACL>
<!--
Root Element 'publicContact' represent collection of public contacts
(containing 1 or more public contacts).A personal contact is owned by an
individual user and is not accessible to all users. A public contact can
be shared by all users and is owned by the default system user.
---company:The organization that the contact belongs to.
---description: A free text field containing human readable text providing
information on this entry.
---displayName:The localized name of a contact to be used when displaying.
It will typically be the localized full name. This value may be provisioned
from the user's enterprise directory entry. If it does not exist,
synchronization rules can be used to populate it for other fields
e.g. Surname, GivenName, or LoginName.
---displayNameAscii:The full text name of the contact represented in ASCII. It is
used to support display (e.g. endpoints) that cannot handle localized text.
---dn:The distinguished name of the user. The DN is a sequence of relative
distinguished names (RDN) connected by commas. An RDN is an attribute with
an associated value in the form of attribute=value, normally expressed in a
UTF-8 string format. The dn can be used to uniquely identify this record.
Note the dn is changeable.
---givenName:The first name of the contact.
---initials:Initials of the contact.
---middleName:The middle name of the contact.
---preferredGivenName:The nick name of the contact.
---preferredLanguage:The individual's preferred written or spoken language.
Values will conform to rfc4646 and the reader should refer to rfc4646 for
syntax.
This format uses the ISO standard Language (ISO-639) and region (ISO-3166)
codes In the absence of a value the client's locale should be used, if no
value is set, en-US should be defaulted.
---source:Free format text field that identifies the entity that created this
user record. The format of this field will be either a IP Address/Port or
a name representing an enterprise LDAP or Avaya.
---sourceUserKey:The key of the user from the source system. If the source is
an Enterprise Active Directory server, this value will be the objectGUID.
---suffix:The text appended to a name e.g. Jr., III.
---surname:The user's last name, also called the family name.
---title:The job function of a person in their organizational context.
Examples: supervisor, manager.
---contactAddresses:A table used to store a contact's address.
---addresses:A fully qualified URI for interacting with this contact.
Any addresses added to this table should contain a qualifier
e.g. sip, sips, tel, mailto. The address should be syntactically valid
based on the qualifier. It must be possible to add via the GUI and
Interface. The application must do validation.
-->
<tns:publicContact>
 <company>ABC</company>
 <description>Company ABC description</description>
 <displayName>John Miller</displayName>

```

```

<displayNameAscii></displayNameAscii>
<dn>dc=acme,dc=org</dn>
<givenName>John</givenName>
<initials>Mr</initials>
<middleName>M</middleName>
<preferredGivenName>John</preferredGivenName>
<preferredLanguage>English</preferredLanguage>
<source>ldap</source>
<sourceUserKey>18966</sourceUserKey>
<suffix>Jr.</suffix>
<surname>Miller</surname>
<title>Manager</title>
<!--
 ---type:The value reflecting the type of handle this is. Possible values
 are "username", "e164", and "privatesubsystem
 ---category:The value representing a further qualification to the contact
 address. Possible values include Office, Home, Mobile.
 ---handle:This is the name given to the user to allow communication to be
 established with the user. It is an alphanumeric value that must comply
 with the userinfo related portion of a URI as described in rfc2396.
 However, it is further restricted as ASCII characters with only the "+"
 prefix to signify this is an E.164 handle and "_" and "." special
 characters supported.The handle and type together are unique within a
 specific domain. Note, the handle plus domain can be used to construct
 a user's Address of Record.
 ---label:A free text description for classifying this contact.
 ---altLabel:A free text description for classifying this contact. This is
 similar to ContactLabel, but it is used to store alternate language
 representations.
-->
 <contactAddresses>
 <contact>
 <type>sip</type>
 <category>office</category>
 <handle>sip:jmiller@abc.com</handle>
 <label>Miller</label>
 <altLabel>John</altLabel>
 </contact>
 </contactAddresses>
<addresses>
<!--
 ---addressType:The unique text name of the address type.
 Possible values are: Home, business.
 ---name: The Name property defines the unique label by which the address is
 known. Default format for user specific address should include user
 name place address type.
 ---building:The name or other designation of a structure.
 ---localityName:The name of a locality, such as a city, county or other
 geographic region.
 ---postalCode:A code used by postal services to route mail to a destination.
 In the United States this is the zip code.
 ---room:Name or designation of a room.
 ---stateOrProvince:The full name of a state or province.
 ---country:A country.
 ---street:The physical address of the object such as an address for package
 delivery
 ---postalAddress:A free formed text area for the complete physical delivery
 address. It may be used in place of the specific fields in this table.
-->
 <address>
 <addressType>office</addressType>
 <name>John Miller</name>
 <building>building A</building>
 <localityName>Magarpatta</localityName>
 <postalCode>411048</postalCode>

```

```

 <room>room 123</room>
 <stateOrProvince>MH</stateOrProvince>
 <country>India</country>
 <street>Hadapsar</street>
 <private>false</private>
 </address>
</addresses>
</tns:publicContact>
<!--
 ---addressType:The unique text name of the address type.
 Possible values are: Home, business.
 ---name: The Name property defines the unique label by which the address is
 known. Default format for user specific address should include user
 name place address type.
 ---building:The name or other designation of a structure.
 ---localityName:The name of a locality, such as a city, county or other
 geographic region.
 ---postalCode:A code used by postal services to route mail to a
 destination. In the United States this is the zip code.
 ---room:Name or designation of a room.
 ---stateOrProvince:The full name of a state or province.
 ---country:A country.
 ---street:The physical address of the object such as an address for package
 delivery
 ---postalAddress:A free formed text area for the complete physical delivery
 address. It may be used in place of the specific fields in this table.
 ---readOnly:A boolean indicator showing whether or not the address can be
 changed from its default value.
-->
<tns:sharedAddress>
 <addressType>office</addressType>
 <name>Avaya Pune</name>
 <building>building A</building>
 <localityName>Magarpatta</localityName>
 <postalCode>411048</postalCode>
 <room>room 123</room>
 <stateOrProvince>MH</stateOrProvince>
 <country>India</country>
 <street>Hadapsar</street>
 <readOnly>true</readOnly>
</tns:sharedAddress>

</tns:globalSettings>

```

## XML Schema Definition for bulk deletion of global setting records

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="http://xml.avaya.com/schema/bulkdelete" targetNamespace="http://
xml.avaya.com/schema/bulkdelete"
 elementFormDefault="qualified" version="1.0" xmlns:xs="http://www.w3.org/
2001/XMLSchema">

 <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"/>
 <xs:element name="publicContact" type="tns:xmlDeletePublicContact" />
 <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry"/>
 <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"/>
 <xs:element name="presenceSystemACL" type="tns:xmlDeletePresSystemACLEntry"/>

 <xs:element name="deleteGlobalSettings">
 <xs:complexType>
 <xs:sequence>

```



```

 <xs:element name="sharedAddress" type="tns:xmlDeleteSharedAddress"
minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="publicContact" type="tns:xmlDeletePublicContact"
minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="presenceEnforcedUserACL"
type="tns:xmlDeletePresEnforcedUserACLEntry" minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="presenceSystemRule" type="tns:xmlDeletePresSystemRule"
minOccurs="0" maxOccurs="unbounded"/>
 <xs:element name="presenceSystemACL" type="tns:xmlDeletePresSystemACLEntry"
minOccurs="0" maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>
</xs:element>

<xs:complexType name="xmlDeleteSharedAddress">
 <xs:sequence>
 <xs:element name="name" type="xs:string" minOccurs="1" maxOccurs="1"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlDeletePublicContact">
 <xs:sequence>
 <xs:element name="displayName" type="xs:string" maxOccurs="1"
minOccurs="1"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlDeletePresEnforcedUserACLEntry">
 <xs:sequence>
 <xs:element name="userName" type="xs:string" maxOccurs="1" minOccurs="1"/>
 <xs:choice>
 <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
 <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
 </xs:choice>
 <xs:element name="priority" type="xs:string" maxOccurs="1" minOccurs="1"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlDeletePresSystemRule">
 <xs:sequence>
 <xs:element name="priority" type="xs:string" maxOccurs="1"
minOccurs="1"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="xmlDeletePresSystemACLEntry">
 <xs:sequence>
 <xs:choice>
 <xs:element name="watcherLoginName" type="xs:string" minOccurs="0"/>
 <xs:element name="watcherDisplayName" type="xs:string" minOccurs="0"/>
 </xs:choice>
 </xs:sequence>
</xs:complexType>
</xs:schema>

```

### Sample XML for bulk deletion of global setting records

```

<?xml version="1.0" encoding="UTF-8"?>
<tns:deleteGlobalSettings xmlns:tns="http://xml.avaya.com/schema/bulkdelete"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://
xml.avaya.com/schema/bulkdelete systemPresence_delete.xsd ">

 <tns:presenceSystemRule>
 <tns:priority>LOW</tns:priority>
 </tns:presenceSystemRule>

```

```

</tns:presenceSystemRule>

 <tns:sharedAddress>
 <tns:name>Avaya Pune</tns:name>
 </tns:sharedAddress>

 <tns:publicContact>
 <tns:displayName>John Miller</tns:displayName>
 </tns:publicContact>

 <tns:presenceEnforcedUserACL>
 <tns:userName>jmiller@avaya.com</tns:userName>
 <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
 <tns:priority>HIGH</tns:priority>
 </tns:presenceEnforcedUserACL>

 <tns:presenceSystemACL>
 <tns:watcherDisplayName>John Miller</tns:watcherDisplayName>
 </tns:presenceSystemACL>
</tns:deleteGlobalSettings>

```

## XML Schema Definition for bulk import of roles

```

<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns="http://xml.avaya.com/bulkimport" xmlns:xs="http://www.w3.org/2001/
XMLSchema" targetNamespace="http://xml.avaya.com/bulkimport"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 This Schema defines schema for bulk import and export of roles.
 Root Element 'Roles' represent collection of role
 (containing 1 or more roles)
 </xs:documentation>
 </xs:annotation>
 <xs:element name="Roles">
 <xs:complexType>
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 A role is a collection of access permissions on a resource.
 A user's role will determine the permissions that the user
 receives to access resources.
 Examples of Roles: Contact Center Manager, Agent,
 Administrator.
 New Roles can be added to the data model using an XML file
 conforming to this XSD.Existing Roles too can be updated.
 </xs:documentation>
 </xs:annotation>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 <xs:element name="Role" maxOccurs="unbounded">
 <xs:complexType>
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 Operation - Element Containing information about the
 Operation.The Operation requires to preexist in
 SMGR database.
 Examples of Operation:
 'UserManagement/GlobalUserSettings/ACL';
 'Settings/Plugin Framework' ;
 Resource - Element Containing information about the
 Resource.
 A Resource can be a User, Role, Operation, Group,
 Element. The Resource requires to preexist in SMGR
 database. Examples of Resource: 'Auditor' ;
 </xs:documentation>
 </xs:annotation>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
</xs:schema>

```

```

 </xs:documentation>
 </xs:annotation>
 <xs:element name="Operation" minOccurs="0" maxOccurs="unbounded">
 <xs:complexType>
 <xs:attribute name="ID" type="xs:string" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ID: The ID of the operation. The value of this tag
 corresponds to the OperationID. Note that it
 is very important that this value is unique
 across the system.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 </xs:complexType>
 </xs:element>
 <xs:element name="Resource" minOccurs="0" maxOccurs="unbounded">
 <xs:complexType>
 <xs:sequence>
 <xs:element name="ResourceAttributes" minOccurs="0"
maxOccurs="unbounded">
 <xs:complexType>
 <xs:attribute name="ID" type="xs:string" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ResourceAttributesID: The ID of the Resource
 Attributes. This specifies the attributes
 of a resource.
 Examples of ResourceAttributesID:
 'ALL' ; 'LoginName' ;
 'First Name' for Resource Type 'user'
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 </xs:complexType>
 </xs:element>
 <xs:element name="Permissions">
 <xs:complexType>
 <xs:sequence>
 <xs:annotation>
 <xs:documentation xml:lang="en">
 Permission: String value specifying Permissions
 that can be assigned to the Resource Type.
 Examples of Permission: view, delete
 </xs:documentation>
 </xs:annotation>
 <xs:element name="Permission" type="xs:string" maxOccurs="unbounded"/>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 </xs:sequence>
 <xs:attribute name="ResourceType" type="xs:string" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ResourceType: String Value for specifying Type
 of the Resource that needs to be imported.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="NativeResourceID" type="xs:string"
use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 NativeResourceID: Native ID of the Resource.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 </xs:sequence>
 </xs:complexType>
 </xs:element>
 </xs:sequence>
</xs:complexType>
</xs:element>

```

```

 </xs:annotation>
 </xs:attribute>
 </xs:complexType>
 </xs:element>
</xs:sequence>
 <xs:attribute name="CanAccessAllOperations" type="xs:boolean"
use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 CanAccessAllOperations - Boolean value specifying
 whether this role can access all operations.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="IsServices" type="xs:boolean" use="required" >
 <xs:annotation>
 <xs:documentation xml:lang="en">
 IsServices - Boolean value specifying whether this
 Role is a Services Role.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="isDefault" type="xs:boolean" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 isDefault - Boolean value specifying whether
 this Role is a System Role. These Roles can
 not be deleted.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="Name" type="xs:string" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 Name - String value specifying Role name.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="AllResourcesPermission" type="xs:string"
use="optional">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 AllResourcesPermission - String value representing
 the comma separated permission strings. These
 permissions will be applied to all Resources
 in the system. The users assigned to this role
 will get the specified permissions for all
 resources.
 Examples of Resource: 'view,delete'
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="Description" type="xs:string" use="optional">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 Description - String value specifying Role
 description.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="isNHIRole" type="xs:boolean" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 isNHIRole - Boolean value specifying whether this
 Role is a non human interface (nhi) role.

```

```

 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="shareRoles" type="xs:boolean" use="optional">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 shareRoles - Boolean value specifying whether this
 Role is a shared role across applications.
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="hasFullAccess" type="xs:boolean" use="optional">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 hasFullAccess - Boolean value specifying full
 access over all resources.
 Examples of Role with full access:
 'System Administrator';
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 <xs:attribute name="ApplicationId" type="xs:string" use="required">
 <xs:annotation>
 <xs:documentation xml:lang="en">
 ApplicationId - The value of this tag corresponds
 to the ApplicationID.
 Examples of ApplicationId: 'SMGR';
 </xs:documentation>
 </xs:annotation>
 </xs:attribute>
 </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

## Sample XML for bulk import of roles

```

<?xml version="1.0" encoding="UTF-8"?>
<!--
 Root Element 'Roles' represent collection of role
 (containing 1 or more roles)
-->
<Roles xsi:schemaLocation="http://xml.avaya.com/bulkimport BulkImport.xsd"
xmlns="http://xml.avaya.com/bulkimport" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
 <!--
 A role is a collection of access permissions on a resource. A user's role
 will determine the permissions that the user receives to access resources.
 ---CanAccessAllOperations: Boolean value specifying whether this role can
 access all operations.
 ---IsServices: Boolean value specifying whether this Role is a Services Role.
 ---isDefault: Boolean value specifying whether this Role is a System Role.
 These Roles can not be deleted.
 ---Name: String value specifying Role name.
 ---AllResourcesPermission:String value representing the comma separated
 permission strings. These permissions will be applied to all
 Resources in the system. The users assigned to this role will get
 the specified permissions for all resources.
 ---Description:String value specifying Role description.
 ---isNHIRole:Boolean value specifying whether this Role is a non human interface
 (nhi) role.
 ---shareRoles: Boolean value specifying whether this Role is a shared role
 across applications.
 -->

```

```

 ---hasFullAccess:Boolean value specifying full access over all resources.
 ---ApplicationId:The value of this tag corresponds to the ApplicationID.
 Examples of ApplicationId: 'SMGR'
 -->
 <Role CanAccessAllOperations="true" IsServices="true" isDefault="false" Name="test-
role" AllResourcesPermission="view,delete" Description="System Administrator Role"
isNHIRole="false" shareRoles="true" hasFullAccess="false"
ApplicationId="SMGR" >
 <!--
 Element Containing information about the Operation.The Operation requires
 to preexist in SMGR database.
 ---ID: The ID of the operation.The value of this tag corresponds to the
 OperationID. Note that it is very important that this value is
 unique across the system
 -->
 <Operation ID="GroupsAndRoles/RBAC/ViewRole"/>
 <!--
 ---Resource : Element Containing information about the Resource.
 A Resource can be a User, Role, Operation, Group,
 Element.The Resource requires to preexist in SMGR
 database.
 ---ResourceType: String Value for specifying Type of the Resource
 that needs to be imported.
 ---NativeResourceID: Native ID of the Resource.
 -->
 <Resource ResourceType="alarmoperation"
NativeResourceID="ChangeStatusAll">
 <!--
 ResourceAttributesID: The ID of the ResourceAttributes.
 This specifies the attributes of a resource
 -->
 <ResourceAttributes ID="ALL" />
 <!--
 ---Permission: String value specifying Permissions that can be
 assigned to the Resource Type.
 -->
 <Permissions>
 <Permission>view</Permission>
 </Permissions>
 </Resource>
 </Role>
</Roles>

```

## Attribute details defined in Import user XSD

| Attribute          | Attribute Description                                                                  | Mandatory/Optional | Validation Constraints                                                                           |
|--------------------|----------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------|
| authenticationType | The type of authentication the user undergoes at runtime to gain access to the system. | Mandatory          | The options are: <ul style="list-style-type: none"> <li>• BASIC</li> <li>• ENTERPRISE</li> </ul> |
| description        | A description of the user. A human readable description of this user instance.         | Optional           |                                                                                                  |

*Table continues...*

| Attribute                | Attribute Description                                                                                                                                                                                                                                                                                                                              | Mandatory/Optional | Validation Constraints |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| displayName              | The localized name of the user to be used when displaying. Typically, the value is the localized full name. This value might be provisioned from the enterprise directory entry of the user. If the value does not exist, you can use synchronization rules to populate the value for other fields. For example: Surname, GivenName, or LoginName. | Optional           |                        |
| displayNameAscii         | The name that corresponds to the console attribute Endpoint Display Name. The full text name of the user represented in ASCII. The attribute used for displaying (e.g. endpoints) the unsupported localized text.                                                                                                                                  | Optional           |                        |
| dn                       | The distinguished name (DN) of the user. DN is a sequence of relative distinguished names (RDN) connected by commas. RDN is an attribute with an associated value in the form of attribute=value, typically expressed in a UTF-8 string format. Use DN for identifying the user and for authentication subject mapping. You can change DN.         | Optional           |                        |
| isDuplicatedLoginAllowed | A boolean that indicates whether this user is allowed a duplicate concurrent logins. true indicates that the user can have duplicate logins.                                                                                                                                                                                                       | Optional           | Default value is true. |

*Table continues...*

| Attribute     | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Mandatory/Optional | Validation Constraints  |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------|
| isEnabled     | A boolean that indicates whether or not the user is active. Users with AuthenticationType=Basic fails if the value is false. This attribute can be used to disable access between login attempts. You cannot revoke login for a running session. Alternatively, the administrator can always modify the password to disable the user from logging in. A true stipulates this is an active user, a false used for a disabled user.                                                                                                                                                                                                                 | Optional           | Default value is false. |
| isVirtualUser | A boolean that indicates whether or not the record is being used for a non-human entity such as an application, service, and software agent. You require this attribute where the entity behaves as a user and needs to have subset of the user profile populated. If the entity does not behave as a user and has a different trust relationship, for example, a trust certificate must not be treated as a virtual user. A virtual user can represent an Avaya or an external non-human entity. This attribute is provided as a convenience to track such accounts. A true stipulates this is a virtual users, a false is used for human users. | Optional           | Default value is false. |
| givenName     | The first name of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Mandatory          |                         |
| honorific     | The personal title used to address a user. This is typically a social title and not the work title which is contained in the title attribute. This attribute can map to PersonalTitle.                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Optional           |                         |

Table continues...



| Attribute          | Attribute Description                                                                                                                                                                               | Mandatory/Optional | Validation Constraints |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| loginName          | The unique login name that you provide for the user. The format for the login name is username@domain. The login name is an alphanumeric value and supports the ASCII characters “_”, “.”, and “-”. | Mandatory          |                        |
| middleName         | The middle name of the user.                                                                                                                                                                        | Optional           |                        |
| managerName        | The name of the manager of the user. This is a free formed field and does not require the user's manager to be a user of the solution. The attribute supports the reporting needs.                  | Optional           |                        |
| preferredGivenName | The preferred first name of the user.                                                                                                                                                               | Optional           |                        |

*Table continues...*

| Attribute         | Attribute Description                                                                                                                                                                                                                                             | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| preferredLanguage | The preferred written or spoken language. The format uses the ISO standard Language (ISO-639) and region (ISO-3166) codes. If a preferred language is not available, the locale of the client must be used. If the value is blank, en_US must be used as default. | Optional           | <p>The options are:</p> <ul style="list-style-type: none"> <li>English (United States) - en_US</li> <li>Chinese (Simplified) - zh_CN</li> <li>Japanese (Japan) - ja_JP</li> <li>Korean (Korea) - ko_KR</li> <li>French (France) - fr_FR</li> <li>German (Germany) - de_DE</li> <li>Italian (Italy) - it_IT</li> <li>Russian (Russia) - ru_RU</li> <li>English (United Kingdom) - en_GB</li> <li>Spanish (Mexico) - es_MX</li> <li>Portuguese (Brazil) - pt_BR</li> <li>French (Canada) - fr_CA</li> <li>English (Canada) - en_CA</li> </ul> |
| source            | A free format text field that identifies the entity that created this user record. The format of this field must be a IP Address/ Port or a name representing an enterprise LDAP or Avaya.                                                                        | Optional           | User Management populates the source field with the name of the file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| sourceUserKey     | The key of the user from the source system. If the source is an Enterprise Active Directory server, the key is objectGUID.                                                                                                                                        | Optional           | By default, the value is none.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table continues...

| Attribute | Attribute Description                                                                                                                                                                                                                                         | Mandatory/Optional | Validation Constraints                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------|
| status    | The information that helps provisioning activities such as correcting or completing the provisioning of a user. It can also signify that approval is needed (PENDINGAUTHZ) before a user account is sufficiently configured to be a valid user (PROVISIONED). | Optional           | The options are:<br>AUTHPENDING;<br>PENDINGAUTHZ;<br>PROVISIONED |
| suffix    | The text appended to a name. For example, Jr., III.                                                                                                                                                                                                           | Optional           |                                                                  |
| surname   | The last name or the family name of the user.                                                                                                                                                                                                                 | Mandatory          |                                                                  |

*Table continues...*

| Attribute | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timeZone  | <p>The preferred time zone of the user. For example: America/New_York, Europe/Dublin. The application consuming this information must know how to translate e.g. in Java it is <code>TimeZone.getTimeZone("Europe/Moscow")</code>; In the absence of a value, the system uses the local services timezone.</p> <p><b>* Note:</b></p> <p>While using the suggested <b>timeZone</b> values, consider daylight saving time (DST) and summer time adjustments. Typically, you add 1 hour to the offset.</p> <p><b>* Note:</b></p> <p>In the import xml files, make the following changes while using specific characters:</p> <ul style="list-style-type: none"> <li>• less-than character (&lt;) as <code>&amp;lt;</code>;</li> <li>• ampersand character (&amp;) as <code>&amp;amp;</code>;</li> <li>• greater-than character (&gt;) as <code>&amp;gt;</code>;</li> <li>• double-quote character (") as <code>&amp;quot;</code>;</li> <li>• apostrophe or single-quote character (') as <code>&amp;apos;</code>;</li> </ul> | Optional           | <p>(-12:0)International Date Line West</p> <p>(-11:0)Midway Island, Samoa</p> <p>(-10:0)Hawaii</p> <p>(-9:0)Alaska</p> <p>(-8:0)Pacific Time (US &amp; Canada); Tijuana</p> <p>(-7:0)Mountain Time (US &amp; Canada); Chihuahua, La Paz</p> <p>(-7:0)Arizona</p> <p>(-6:0)Central Time (US &amp; Canada); Guadalajara, Mexico City</p> <p>(-6:0)Central America; Saskatchewan</p> <p>(-5:0)Indiana (East); Bogota, Lima, Quito</p> <p>(-5:0)Eastern Time (US &amp; Canada)</p> <p>(-4:0)Caracas, La Paz</p> <p>(-4:0)Atlantic Time (Canada); Santiago, Manaus</p> <p>(-3:30)Newfoundland</p> <p>(-3:0)Georgetown</p> <p>(-3:0)Brasilia, Greenland, Buenos Aires, Montevideo</p> <p>(-2:0)Mid-Atlantic</p> <p>(-1:0)Azores</p> <p>(-1:0)Cape Verde Is.</p> <p>(0:0)Monrovia, Reykjavik</p> |

*Table continues...*

| Attribute | Attribute Description | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                       |                    | (0:0)GMT : Dublin,<br>Edinburgh, Lisbon,<br>London, Casablanca<br><br>(+1:0)West Central<br>Africa<br><br>(+1:0)Amsterdam,<br>Berlin, Rome,<br>Belgrade, Prague,<br>Brussels, Sarajevo<br><br>(+2:0)Harare, Pretoria<br><br>(+2:0)Amman, Athens,<br>Minsk, Beirut, Cairo,<br>Jerusalem, Helsinki,<br>Windhoek<br><br>(+3:0)Baghdad, Kuwait,<br>Riyadh, Nairobi, Tbilisi<br><br>(+3:0)Moscow, St.<br>Petersburg, Volgograd<br><br>(+3:30)Tehran<br><br>(+4:0)Abu Dhabi,<br>Muscat, Caucasus<br>Standard Time<br><br>(+4:0)Baku, Tbilisi,<br>Yerevan<br><br>(+4:30)Kabul<br><br>(+5:0)Islamabad,<br>Karachi, Tashkent,<br>Ekaterinburg<br><br>(+5:30)Chennai,<br>Kolkata, Mumbai, New<br>Delhi, Sri<br>Jayawardenepura<br><br>(+5:45)Kathmandu<br><br>(+6:0)Astana, Dhaka,<br>Almaty, Novosibirsk<br><br>(+6:30)Rangoon<br><br>(+7:0)Bangkok, Hanoi,<br>Jakarta, Krasnoyarsk |

*Table continues...*

| Attribute | Attribute Description                                                                                                                                                                                                                                                                                      | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                                                                                                                                                                                                                                                                                                            |                    | (+8:0)Beijing, Hong Kong, Singapore; Taipei<br>(+8:0)Perth; Irkutsk, Ulaan Bataar<br>(+9:0)Seoul, Osaka, Sapporo, Tokyo<br>(+9:0)Yakutsk<br>(+9:30)Darwin, Adelaide<br>(+10:0)Brisbane, Guam, Port Moresby<br>(+10:0)Canberra, Melbourne, Sydney, Hobart, Vladivostok<br>(+11:0)Magadan, Solomon Is., New Caledonia<br>(+12:0)Auckland, Wellington<br>(+12:0)Fiji, Kamchatka, Marshall Is.<br>(+13:0)Nuku'alofa |
| title     | The job function of a person in their organizational context.                                                                                                                                                                                                                                              | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                 |
| userName  | The username portion of the loginName field. An alphanumeric value that must comply with the userinfo related portion of a URI as described in rfc2396. However, it is further restricted as ASCII characters with only the _, -, and . special characters supported. This is the rfc2798 "uid" attribute. | Mandatory          |                                                                                                                                                                                                                                                                                                                                                                                                                 |

*Table continues...*

| Attribute         | Attribute Description                                                                                                                                                                                                                                           | Mandatory/Optional | Validation Constraints                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------|
| userPassword      | The encrypted password for this user account. A null password is used when the user is authenticated by the enterprise such as with a separate source such as the enterprise LDAP.                                                                              | Optional           | Need not specified value for Enterprise User. If the value is not specified for the Basic user, the user will be disabled. |
| commPassword      | The encrypted “subscriber” or communication password with which the user logs can use to authentication with on to any CommProfile SIP and non SIP. This attribute is shared across different communication profiles and thus different communication services. | Optional           |                                                                                                                            |
| userType          | The possible primary user application types. A User can be associated with multiple user types.                                                                                                                                                                 | Optional           | The options are administrator, communication_user, agent, supervisor, resident_expert, service_technician, lobby_phone     |
| roles             | The text name of a role. This value must be available in the System Manager database.                                                                                                                                                                           | Optional           |                                                                                                                            |
| address           | The address of the user.                                                                                                                                                                                                                                        | Optional           |                                                                                                                            |
| securityIdentity  | The SecurityIdentity is used to hold any additional identities for a user that can be used for authentication such as loginName, Kerberos account name, or X509 certificate name.                                                                               | Optional           |                                                                                                                            |
| ownedContactLists | It is a collection of internal or external contacts. ContactList is owned by a specific user and has a name that a unique name within the context of its owner.                                                                                                 | Optional           | The system creates a default contactlist per user.                                                                         |

Table continues...

| Attribute             | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                      | Mandatory/Optional | Validation Constraints                |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------|
| ownedContacts         | A non-Avaya application user (external) contact. Contacts can be collected together along with User entities into a contact list. Contacts can be created by an administrator or an end user.                                                                                                                                                                                                              | Optional           |                                       |
| presenceUserDefault   | The personal rules that are set by presentities to define how much presence information can be shown to watchers that are not explicitly mentioned in an ACL. There can be one User Default rule per presentity (User), or none.                                                                                                                                                                           | Optional           |                                       |
| presenceUserACL       | The personal rules defined by presentities themselves on who can monitor their presence information. There might be several entries in the list for a given presentity, each entry corresponding to one watcher.                                                                                                                                                                                           | Optional           |                                       |
| presenceUserCLDefault | The personal rule that is set by presentities to define how much presence information can be shown to watchers that belong to the contact list of the user. There can be one User Contact List Default rule per presentity (Person) or none.                                                                                                                                                               | Optional           |                                       |
| commProfileSet        | The default Commprofile set of the user. A commprofile set can exist without any handles or commprofiles referencing it. That is, you can create a commprofile set without creating a handle or a commprofile. A commprofile set can contain multiple commprofiles, but only one of each specific type. This is enforced by having the CommProfile uniqueness constraint include type, commprofile_set_id. | Optional           | A user has a default commprofile set. |

*Table continues...*



| Attribute      | Attribute Description                           | Mandatory/Optional | Validation Constraints |
|----------------|-------------------------------------------------|--------------------|------------------------|
| employeeNo     | The employee number of the user.                | Optional           |                        |
| department     | The department which the employee belongs to.   | Optional           |                        |
| organization   | The organization which the employee belongs to. | Optional           |                        |
| localizedNames | The localized name of the user.                 | Optional           |                        |

## Attribute details defined in Delete User XSD

| Attribute  | Attribute description                                                                                                                                                                                                                                                                                                                                                   | Mandatory/Optional | Validation constraints                                                                                |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------|
| deleteType | <p>Defines the delete type of the user. If the user selects:</p> <ul style="list-style-type: none"> <li>• soft: The system does not delete the user record permanently. You can recover the user record.</li> <li>• permanent: The system permanently deletes all attributes associated with the user and the links to public contacts and shared addresses.</li> </ul> | Mandatory          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• soft</li> <li>• permanent</li> </ul> |
| loginName  | A unique system login name assigned to the user in the format username@domain or username.                                                                                                                                                                                                                                                                              | Mandatory          |                                                                                                       |
| id         | A unique identifier for a user record. The id attribute is included in the XSD for future enhancement. This is not used in System Manager the current release.                                                                                                                                                                                                          | Optional           |                                                                                                       |

## Attribute details defined in the CM Endpoint profile XSD

### Attribute details defined in the CM Endpoint profile XSD

| Attribute                                      | Attribute Description                                                                                                                     | Mandatory/Optional | Validation Constraints |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| CM Name<br>cmName                              | The name of the Communication Managementsystem as it appears in the Applications/Application Management/Entities.                         | Mandatory          |                        |
| Use Existing Extension<br>useExistingExtension | Select <b>true</b> if you want to use an already created extension.<br><br>Select <b>false</b> if you want to use an available extension. | Optional           |                        |
| Template Name<br>template                      | The template name that is used to create the endpoint. Values defined in the template will be used if you do not provide other values.    | Optional           |                        |
| Set Type<br>setType                            | The set type of the endpoint.                                                                                                             | Optional           |                        |

*Table continues...*

| Attribute    | Attribute Description | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port<br>port | The valid port value. | Optional           | <p>01 to 64 First and second numbers are the cabinet numbers having values A to E. The third character is the carrier having values between 01 to 20. Fourth and fifth characters are the slot number between 01 to 32. Sixth and seventh characters are the circuit number having values x or X.</p> <p>Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set, or that the extension had a non-IP set, and is dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) endpoints, as well as for SBS Extensions.</p> <p>IP Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has an IP set. This is autopopulated for certain IP endpoint set types. You can enter the value for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.</p> |

*Table continues...*

| Attribute                                         | Attribute Description                                                                                                                                                                                   | Mandatory/Optional | Validation Constraints                                                                 |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------|
| Delete endpoint is unassigned<br>deleteOnUnassign | Specifies whether the endpoint must be deleted if it is unassigned from the user.                                                                                                                       | Optional           |                                                                                        |
| Lock messages feature.<br>lockMessages            | Select to enable the lock messages feature.                                                                                                                                                             | Optional           | Select true or false to enable or disable the lock messages feature respectively.      |
| Coverage Path 1<br>coveragePath1                  | A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.                                                                                       | Optional           | Valid values: Path Number between 1-9999, time of day table between t1-t999, or blank. |
| Coverage Path 2                                   | A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.                                                                                       | Optional           | Valid values: Path Number between 1-9999, time of day table between t1-t999, or blank. |
| Hunt To Station<br>huntToStation                  | The extension the system must hunt to for this telephone when the telephone is busy. A endpoint hunting chain can be created by assigning a hunt-to endpoint to a series of telephones.                 | Optional           |                                                                                        |
| Tenant Number<br>tn                               | Provides partitioning of attendant groups and endpoints and trunk groups.<br><br>Typically this is used for multiple tenants in a building or multiple departments within a company or an organization. | Mandatory          | Valid values: 1 to 250                                                                 |
| Class of Restriction<br>cor                       | This is used for multiple tenants in a building or multiple departments within a company or an organization.                                                                                            | Mandatory          | Valid values: 0 to 995                                                                 |

*Table continues...*

| Attribute                                                  | Attribute Description                                                                                                                                                                                                                                                                       | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Class of Service<br>cos                                    | Class of Service lets you define a group of users and control the groups' access to features.                                                                                                                                                                                               | Mandatory          | Valid values: 0 to 15                                                                                                                                                                                                                                                                                                                |
| speakerphone                                               | Controls the behavior of speakerphones.                                                                                                                                                                                                                                                     | Optional           | Valid values : none, 1-way, 2-way                                                                                                                                                                                                                                                                                                    |
| Display Language<br>displayLanguage                        | The language that displays on the endpoint.                                                                                                                                                                                                                                                 | Optional           | Time of day is displayed in the 24- hour format (00:00 - 23:59) for all languages except English, which is displayed in the 12-hour format (12:00 a.m. to 11:59 p.m.).<br><br>unicode: Displays English messages in a 24-hour format . If you do not install the Unicode file, the endpoint displays messages in English by default. |
| Personalized Ringing Pattern<br>personalizedRingingPattern | The personalized ringing pattern for the endpoint.<br><br>Personalized Ringing allows the users of some telephones to have one of the eight ringing patterns for incoming calls.<br><br>For virtual endpoints, this field dictates the ringing pattern on its mapped to physical telephone. |                    | L = 530 Hz, M = 750 Hz, and H = 1060 Hz<br><br>Valid Entries Usage:<br><ol style="list-style-type: none"> <li>1. MMM (standard ringing)</li> <li>2. HHH</li> <li>3. LLL</li> <li>4. LHH</li> <li>5. HHL</li> <li>6. HLL</li> <li>7. HLH</li> <li>8. LHL</li> </ol>                                                                   |
| Message Lamp Extension<br>messageLampExt                   | The Message Lamp Extension associated with the current extension.                                                                                                                                                                                                                           | Mandatory          |                                                                                                                                                                                                                                                                                                                                      |
| muteButtonEnabled                                          | Select to enable the mute button on the endpoint.                                                                                                                                                                                                                                           |                    |                                                                                                                                                                                                                                                                                                                                      |

Table continues...

| Attribute                                  | Attribute Description                                                                                                                                                                                                                                                                                     | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Media Complex Extension<br>mediaComplexExt | When used with Multi-media Call Handling, this field indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to either place a voice or a data call. Voice conversion, coverage, and forwarding apply as if the call were made to the 1-number. | Optional           | Valid Entry Usage: A valid BRI data extension. For MMCH, enter the extension of the data module that is part of this multimedia complex.<br><br>H.323 endpoint extension: For the 4600 series IP Telephones, enter the corresponding H.323 endpoint. For IP Softphone, enter the corresponding H.323 endpoint. If you enter a value in this field, you can register this endpoint on either a road-warrior or elecommuter/Avaya IP Agent application.<br><br>Blank: Leave this field blank for single-connect IP applications. |
| IP Softphone<br>ipSoftphone                | Specifies whether the endpoint is an IP soft phone.                                                                                                                                                                                                                                                       | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

*Table continues...*

| Attribute                                       | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Mandatory/Optional | Validation Constraints                                                                  |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------|
| Servivable GK Node Name<br>servivableGkNodeName | <p>Servivable GK Node Name identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the H.248 gateways.</p> <p>When you enter a valid IP node name in this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP endpoints register with Communication Manager, this list is sent to the registration confirm message. The IP endpoint can use the IP address of this Survivable Gatekeeper as the call controller of last resort to register with. Survivable GK Node Name is available only if the endpoint is an H.323 endpoint (46xx or 96xx set types).</p> | Optional           | Valid Entry Usage: Valid IP node name, any valid, previously-administered IP node name. |

*Table continues...*

| Attribute                                        | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Survivable class of restriction<br>survivableCOR | Sets the level of restriction for endpoints to be used with the survivable dial plan to limit certain users to certain types of calls. You can list the restriction levels from the most restrictive to least restrictive. Each level assumes the calling ability of the ones above it. This field is used by the PIM module in Integrated Management to communicate with the Communication Manager administration tables and to obtain the class of service information. PIM module builds a managed database to send to Standard Local Survivability (SLS) on the H.248 gateways. Survivable COR is valid for all analog and IP endpoint types. | Optional           | <p>Valid Entries: Usage emergency - This endpoint can only be used to place emergency calls.</p> <p>Internal - This endpoint can only make intra-switch calls. This is the default value.</p> <p>local - This endpoint can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.</p> <p>toll - This endpoint can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.</p> <p>unrestricted - This endpoint can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.</p> |

*Table continues...*



| Attribute                                           | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Survivable Trunk Destination<br>survivableTrunkDest | This field does not allow certain telephones to receive incoming trunk calls when the media gateway is in survivable mode. This field is used by the PIM module in Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the H.248 gateways. Survivable Trunk Destination is available for all analog and IP endpoint types. | Optional           | Valid Entry Usage:<br><br>true - Allows this endpoint to be an incoming trunk destination while the media gateway is running in the survivability mode. This is the default value.<br><br>false - Prevents this endpoint from receiving incoming trunk calls when the endpoint in survivable mode. |
| Voice Mail Number<br>voiceMailNumber                | Enter the complete Voice Mail Dial Up number.                                                                                                                                                                                                                                                                                                                                                                                                                                 | Optional           | String                                                                                                                                                                                                                                                                                             |
| offPremisesStation                                  | Analog telephones only.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Optional           | Valid entries Usage:<br><br>• true - Enter true if this telephone is not located in the same building as the system. If you enter true, you must complete the R Balance Network.<br><br>• false - Enter false if the telephone is located in the same building as the system.                      |
| dataOption                                          | If a second line on the telephone is administered on the I-2 channel, enter <i>analog</i> . Else, enter the data module if applicable, or enter <i>none</i> .                                                                                                                                                                                                                                                                                                                 | Optional           | Valid entries: analog, none.                                                                                                                                                                                                                                                                       |

Table continues...

| Attribute                                            | Attribute Description                                                                                                                                                                                                                                                                                                                         | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message Waiting Indicator<br>messageWaitingIndicator | If you select led or neon, then you must enable messageLampExt, else leave this field blank.                                                                                                                                                                                                                                                  | Optional           | Valid entries: led, neon, none.                                                                                                                                                                                                                                                                             |
| remoteOfficePhone                                    | Select <b>true</b> to use this endpoint as an endpoint in a remote office configuration.                                                                                                                                                                                                                                                      | Optional           | Valid entries: <ul style="list-style-type: none"> <li>• audix - If LWC is attempted, the messages are stored in AUDIX.</li> <li>• spe - If LWC is attempted, the messages are stored in the system processing element (spe).</li> <li>• none - If LWC is attempted, the messages are not stored.</li> </ul> |
| lwcActivation                                        | Select true to allow internal telephone users to leave short LWC messages for this extension. If the system has hospitality, select true for guest-room telephones for the designated extensions to receive failed wakeup messages, and to receive LWC messages that indicate the wakeup calls failed. Select true if LWC Reception is audix. | Optional           | Boolean                                                                                                                                                                                                                                                                                                     |
| activeStationRinging                                 | Active endpoint ringing                                                                                                                                                                                                                                                                                                                       | Optional           | Valid entries: <ul style="list-style-type: none"> <li>• single</li> <li>• continuous</li> <li>• if-busy-single</li> <li>• silent</li> </ul>                                                                                                                                                                 |

Table continues...

| Attribute          | Attribute Description                                                                                   | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| idleActiveRinging  | Defines how a call rings to the telephone when it is on-hook.                                           | Optional           | Valid entries <ul style="list-style-type: none"> <li>• continuous - Select continuous to cause all calls to this telephone to ring continuously.</li> <li>• if-busy-single - Select if-busysingle to cause calls to this telephone to ring continuously when the telephone is off-hook and idle, and calls to this telephone to receive one ring cycle and then ring silently when the telephone is off-hook and active.</li> <li>• silent-if-busy - Select silent-if-busy to cause calls to ring silently when this endpoint is busy.</li> <li>• single - Select single to cause calls to this telephone to receive one ring cycle and then ring silently.</li> </ul> |
| switchhookFlash    | Set this field to true when the <b>Type</b> field is set to H.323.                                      | Optional           | Boolean                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ignoreRotaryDigits | If you set this field to true, the short switch-hook flash (50 to 150) from a 2500-type set is ignored. | Optional           | Boolean                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

*Table continues...*

| Attribute      | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Mandatory/Optional | Validation Constraints |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| h320Conversion | H.320 Conversion — Valid entries are true and false (default). This field is optional for non-multimedia complex voice endpoints and for basic multimedia complex voice endpoints. H.320 Conversion is mandatory for enhanced multimedia complex voice endpoints. Since the system can only handle a limited number of conversion calls, you must limit the number of telephones with H.320 conversion. Enhanced multimedia complexes must have this flag set to true. | Optional           | Boolean                |

*Table continues...*

| Attribute       | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Mandatory/Optional | Validation Constraints             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------|
| serviceLinkMode | <p>The service link is the combined hardware and software multimedia connection between an Enhanced mode complex's H.320 DVC system and the Avaya DEFINITY Server which ends the H.320 protocol. A service link is never used by a Basic mode complex H.320 DVC system. Connecting a service link will take several seconds. When the service link is connected, it uses MMI, VC and system timeslot resources. When the service link is disconnected it does not tie up any resource. Service Link Mode can be administered as either as-needed or permanent:</p> <ul style="list-style-type: none"> <li>• As- Needed - Most non-call center multimedia users will be administered with this service link mode. The as-needed mode provides the enhanced multimedia complex with a connected service link whenever a multimedia call is answered by the endpoint and for a period of 10 seconds after the last multimedia call on the endpoint has been disconnected. Having the service link stay connected for 10 seconds allows a user</li> </ul> | Optional           | Valid entries: as-needed permanent |

*Table continues...*

| Attribute | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Mandatory/Optional | Validation Constraints |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
|           | <p>to disconnect a multimedia call and then make another multimedia call without having to wait for the service link to disconnect and reestablish.</p> <ul style="list-style-type: none"> <li>• Permanent – Multimedia call center agents and other users who are constantly making or receiving multimedia calls might want to be administered with this service link mode.</li> </ul> <p>The permanent mode service link will be connected during the endpoint's first multimedia call and will remain in a connected state until the user disconnects from their PC's multimedia application or the Avaya DEFINITY Server restarts. This provides a multimedia user with a much quicker video cut-through when answering a multimedia call from another permanent mode endpoint or a multimedia call that has been early answered.</p> |                    |                        |

*Table continues...*

| Attribute         | Attribute Description                                                                                              | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| multimediaMode    | There are two multimedia modes, Basic and Enhanced.                                                                | Optional           | <p>Basic - A basic multimedia complex consists of a BRIconnected multimedia-equipped PC and a non-BRI-connected multifunction telephone set.</p> <p>Enhanced - An enhanced multimedia complex consists of a BRI-connected multimediaequipped PC and a non-BRIconnected multifunction telephone.</p>                                                                                                                                                                                                                                                                           |
| mwiServedUserType | Controls the auditing or interrogation of a served user's message waiting indicator (MWI).                         | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. fp-mwi - Select this option if the endpoint is a served user of an fp-mwi message center.</li> <li>2. qsig-mwi - Select this option if the endpoint is a served user of a qsig-mwi message center.</li> <li>3. sip adjuncts - Select this option if the endpoint is a served user of a sip adjunct message center.</li> <li>4. blank - Leave this field blank if you do not want to audit the served user's MWI or if the user is not a served user of either an fp-mwi or qsigmwi message center.</li> </ol> |
| audixName         | The AUDIX associated with the endpoint. Must contain a user-defined adjunct name that was previously administered. | Optional           | String                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

Table continues...

| Attribute      | Attribute Description                                                                                                                                                                                                                       | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| automaticMoves | Automatic Moves allows a DCP telephone to be unplugged from one location and moved to a new location without additional Communication Manager administration. Communication Manager automatically associates the extension to the new port. | Optional           | Valid entries: <ol style="list-style-type: none"> <li>1. always - Select always to move the DCP telephone anytime without additional administration by unplugging the telephone from one location and plugging it into a new location.</li> <li>2. once - Select once to unplug and plug the DCP telephone into a new location once. After a move, the field is set to done the next time that routine maintenance runs on the DCP telephone. Use once when you want to move a large number of DCP telephones so that each extension is removed from the move list. Use once to prevent automatic maintenance replacement.</li> <li>3. no - Enter no to require administration in order to move the DCP telephone.</li> <li>4. done - Done is a display-only value. Communication Manager sets the field to done after the telephone is moved and routine maintenance runs</li> </ol> |

*Table continues...*



| Attribute                     | Attribute Description                                                                                                                                                                                                  | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               |                                                                                                                                                                                                                        |                    | <p>on the DCP telephone.</p> <p>5. Error - Error is a display-only value. Communication Manager sets the field to error, after routine maintenance runs on the DCP telephone, when a non-serialized telephone is set as a movable telephone.</p>                                                                                                                                                                                                                                                                                                                                            |
| remoteSoftphoneEmergencyCalls | An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. As-on-local: As-on-local sends the extension entered in the Emergency Location Extension field on the Endpoint screen to the Public Safety Answering Point (PSAP)</li> <li>2. Block - Block prevents the completion of emergency calls.</li> <li>3. Cesid - Cesid allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP.</li> <li>4. Option - Option allows the user to select the option (extension, block, or cesid) that the user selected during registration.</li> </ol> |

*Table continues...*

| Attribute            | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Mandatory/Optional | Validation Constraints |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| emergencyLocationExt | <p>This field allows the system to properly identify the location of a caller who dials a 911 emergency call from this endpoint. An entry in this field must be of an extension type included in the dial plan, but does not have to be an extension on the local system. The entry can be a UDP extension.</p> <p>The default entry is blank. A blank entry typically is used for an IP softphone dialing in through PPP from somewhere outside your network. If you populate the IP Address Mapping screen with emergency numbers, the feature functions as follows. If the Emergency Location Extension field in the Endpoint screen is the same as the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension to the Public Safety Answering Point (PSAP). If the Emergency Location Extension field in the Endpoint screen is different from the Emergency Location Extension field in the IP Address Mapping screen, the feature sends the extension in the IP Address Mapping screen to the Public</p> | Optional           |                        |

*Table continues...*

| Attribute             | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Mandatory/Optional | Validation Constraints |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
|                       | Safety Answering Point (PSAP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                    |                        |
| alwaysUse             | A softphone can register no matter what emergency call handling settings the user has entered in the softphone. If a softphone dials 911, the administered Emergency Location Extension is used. The softphone's user-entered settings are ignored. If an IP telephone dials 911, the administered Emergency Location Extension is used. If a call center agent dials 911, the physical endpoint extension is displayed, overriding the administered LoginID for ISDN Display. This does not apply to SCCAN wireless telephones, or to extensions administered as type h.323. | Optional           | Boolean                |
| precedenceCallWaiting | Activates or deactivates Precedence Call Waiting for this endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Optional           |                        |

*Table continues...*

| Attribute                   | Attribute Description                                                                                                                                                                                                                                                                                                                                                          | Mandatory/Optional | Validation Constraints |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| autoSelectAnyIdleAppearance | Enables or disables automatic selection of any idle appearance of transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Optional Boolean Communication Manager selects the first idle appearance coverageMsgRetrieval. | Optional           | Boolean                |
| coverageMsgRetrieval        | Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.                                                                                                                                                                                          | Optional           | Boolean                |

*Table continues...*

| Attribute  | Attribute Description                                                                                                       | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| autoAnswer | In EAS environments, the auto answer setting for the Agent LoginID can override a endpoint's setting when an agent logs in. | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. all: All ACD and non-ACD calls ended to an idle endpoint cut through immediately. Does not allow automatic hands-free answer for intercom calls. With non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when the Allow Ringer-off with Auto-Answer is enabled for the system.</li> <li>2. acd: Only ACD split /skill calls and direct agent calls to auto answer. Non-ACD calls ended to an endpoint ring audibly. For analog endpoints, the endpoint is off-hook and idle, only the ACD split/skill calls and direct agent calls auto answer; non-ACD calls receive busy treatment. If the endpoint is active on an ACD call and a non-ACD call arrives, the Agent receives call-waiting tone.</li> <li>3. none: All calls ended to this endpoint receive an</li> </ol> |

*Table continues...*

| Attribute                | Attribute Description                                                                                                                                                                                                                                                                                                                                            | Mandatory/Optional | Validation Constraints                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          |                                                                                                                                                                                                                                                                                                                                                                  |                    | audible ringing treatment.<br><br>4. icom: Allows a telephone user to answer an intercom call from the same intercom group without pressing the intercom button.                                |
| dataRestriction          | Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Data restriction cannot be assigned if Auto Answer is administered as all or acd. If enabled, whisper page to this endpoint is denied. | Optional           |                                                                                                                                                                                                 |
| idleAppearancePreference | Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.                                                                                                                                                                                                                                                       | Optional           | true - The user connects to an idle call appearance instead of the ringing call.<br><br>false - The Alerting Appearance Preference is set and the user connects to the ringing call appearance. |
| callWaitingIndication    | Enable or disable call waiting for this endpoint.                                                                                                                                                                                                                                                                                                                | Optional           |                                                                                                                                                                                                 |
| attCallWaitingIndication | Attendant call waiting allows attendant-originated or attendant-extended calls to a busy single-line telephone to wait and sends distinctive call-waiting tone to the single-line user. Select to enable or disable attendant call waiting                                                                                                                       | Optional           | Boolean                                                                                                                                                                                         |

*Table continues...*

| Attribute               | Attribute Description                                                                                                                                                                                              | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| distinctiveAudibleAlert | Select true so that the telephone can receive the three different types of ringing patterns which identify the type of incoming calls.<br>Distinctive ringing might not work properly for off-premises telephones. | Optional           |                                                                                                                                                                                                                                                             |
| restrictLastAppearance  |                                                                                                                                                                                                                    | Optional           | Valid entries:<br><br>1. true: Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only.<br><br>2. false: Last idle call appearance is used for incoming priority calls and outgoing call originations. |

*Table continues...*

| Attribute          | Attribute Description                  | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|----------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adjunctSupervision | Enable or disable Adjunct Supervision. | Optional           | Valid entries: <ol style="list-style-type: none"> <li>1. true: Analog disconnect signal is sent automatically to the port after a call ends. Analog devices such as answering machines and speakerphones use this signal to turn the devices off after a call ends.</li> <li>2. false: Hunt group agents are alerted to incoming calls. In a hunt group environment, the disconnect signal blocks the reception of zip tone and incoming call notification by an auto-answer endpoint when a call is queued for the endpoint.</li> </ol> |

*Table continues...*



| Attribute                      | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                         | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| perStationCpnSendCallingNumber | Send Calling Number                                                                                                                                                                                                                                                                                                                                                                                                                           | Optional           | Valid entries:<br><ol style="list-style-type: none"> <li>1. y: All outgoing calls from the endpoint will deliver the Calling Party Number (CPN) information as Presentation Allowed.</li> <li>2. n: No CPN information is sent for the call.</li> <li>3. r: Outgoing non-DCS network calls from the endpoint will deliver the Calling Party Number information as Presentation Restricted.</li> </ol> |
| busyAutoCallbackWithoutFlash   | Appears on the Endpoint screen for analog telephones, only if the Without Flash field in the ANALOG BUSY AUTO CALLBACK section of the Feature-Related System Parameters screen is set to true. The Busy Auto Callback without Flash field then defaults to true for all analog telephones that allow Analog Automatic Callback. Set this field to true to provide automatic callback for a calling analog endpoint without flashing the hook. | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                       |
| audibleMessageWaiting          | Provides audible message waiting                                                                                                                                                                                                                                                                                                                                                                                                              | Optional           | Boolean                                                                                                                                                                                                                                                                                                                                                                                               |

Table continues...

| Attribute                | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Mandatory/Optional | Validation Constraints |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| displayClientRedirection | <p>Only administrable if Hospitality is enabled on the System Parameters Customer- Options (Optional Features) screen. This field affects the telephone display on calls that originate from an endpoint with Client Room Class of Service.</p> <p>For endpoints with an audix endpoint type, AUDIX Voice Power ports, or ports for any other type of messaging that needs display information, Display Client Redirection must be enabled. Set this field to true to redirect information for a call originating from a Client Room and ending to this endpoint displays.</p> | Optional           | Boolean                |

*Table continues...*

| Attribute                 | Attribute Description                                                          | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| selectLastUsedAppearance  |                                                                                | Optional           | <p>Valid entries:</p> <ol style="list-style-type: none"> <li>1. True: Indicates that an endpoint's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. If you select true, the line selection on an on-hook endpoint only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call.</li> <li>2. false: The line selection on an on-hook endpoint with no alerting calls can be moved to a different line button, which might be serving a different extension.</li> </ol> |
| coverageAfterForwarding   | Specifies whether an unanswered forwarded call is provided coverage treatment. | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| directIpAudioConnections  | Select to allow or deny direct audio connections between IP endpoints.         | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ipAudioHairpinning        | Allows IP endpoints to be connected through the server's IP circuit pack.      | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| primeAppearancePreference | Set prime appearance preference.                                               | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

*Table continues...*

| Attribute        | Attribute Description                                           | Mandatory/Optional | Validation Constraints                          |
|------------------|-----------------------------------------------------------------|--------------------|-------------------------------------------------|
| endpointSiteData | This is applicable for Site Data fields                         |                    |                                                 |
| room             | This is a Site Data field.                                      | Optional           | Max length 10                                   |
| jack             | This is a Site Data field.                                      | Optional           | Max length 5                                    |
| cable            | This is a Site Data field.                                      | Optional           | Max length 5                                    |
| floor            | This is a Site Data field.                                      | Optional           |                                                 |
| building         | This is a Site Data field.                                      | Optional           |                                                 |
| headset          | This is a Site Data field.                                      | Optional           |                                                 |
| speaker          | This is a Site Data field.                                      | Optional           |                                                 |
| mounting         | This is a Site Data field.                                      | Optional           | Valid values d, w.                              |
| cordLength       | This is a Site Data field.                                      | Optional           | Valid range from 0 to 99.                       |
| setColor         | This is a Site Data field.                                      | Optional           |                                                 |
| abbrList         | This is applicable for Station Abbreviated Dialing Data fields. | Optional           |                                                 |
| listType         | This is a Station Abbreviated Dialing Data field.               | Mandatory          | Valid values enhanced, group, personal, system. |
| number           | This is a Station Abbreviated Dialing Data field.               | Mandatory          | A number.                                       |
| buttons          | This is applicable for button data.                             | Optional           |                                                 |
| Number           | This is a button data field.                                    | Mandatory          |                                                 |
| Type             | This is a button data field.                                    | Optional           |                                                 |
| data1            | This is a button data field.                                    | Optional           |                                                 |
| data2            | This is a button data field.                                    | Optional           |                                                 |
| data3            | This is a button data field.                                    | Optional           |                                                 |
| data4            | This is a button data field.                                    | Optional           |                                                 |
| data5            | This is a button data field.                                    | Optional           |                                                 |
| data6            | This is a button data field.                                    | Optional           |                                                 |

Table continues...

| Attribute                  | Attribute Description                  | Mandatory/Optional | Validation Constraints                                               |
|----------------------------|----------------------------------------|--------------------|----------------------------------------------------------------------|
| endpointDataModule         | This is a Station Data module field.   | Optional           |                                                                      |
| dataExtension              | This is a Station Data module field.   | Mandatory          |                                                                      |
| name                       | This is a Station Data module field.   | Optional           | Max length 29                                                        |
| Class of restriction cor   | This is a Station Data module field.   | Mandatory          | Valid range from 0 to 995.                                           |
| Class of Service Cos       | This is a Station Data module field.   | Mandatory          | Valid range from 0 to 15.                                            |
| itc                        | This is a Station Data module field.   | Mandatory          | Valid values:<br>1. restricted<br>2. unrestricted                    |
| Tenant Number              | This is a Station Data module field.   | Mandatory          | Valid range from 1 to 100.                                           |
| listType                   | This is a Station Data module field.   | Optional           | Valid values:<br>1. enhanced<br>2. group<br>3. personal<br>4. system |
| listId                     | This is a Station Data module field.   | Optional           |                                                                      |
| specialDialingOption       | This is a Station Data module field.   | Optional           | Valid values:<br>1. default<br>2. hot-line                           |
| specialDialingAbbrDialCode | This is a Station Data module field.   | Optional           |                                                                      |
| hotLineDestAbbrevList      | This is a Station Hot Line Data field. | Optional           | Valid range 1 to 3                                                   |
| hotLineAbbrevDialCode      | This is a Station Hot Line Data field. | Optional           | Numeric string                                                       |
| nativeName                 | This is a Native Name Data field.      | Optional           |                                                                      |

Table continues...

| Attribute                                           | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Mandatory/Optional | Validation Constraints |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| locale                                              | <p>This is a Native Name Data field.</p> <p> <b>Note:</b></p> <p>If the <b>displayName</b>, <b>givenName</b>, or <b>surname</b> contains characters of multiple scripts then the locale tag should be present.</p> <p>The locale for the multiscrypt languages are:</p> <ul style="list-style-type: none"> <li>• Japanese: <b>ja</b></li> <li>• Simplified Chinese: <b>zh-cn</b></li> <li>• Traditional Chinese: <b>zh-tw</b></li> <li>• Korean: <b>ko-kr</b></li> <li>• Vietnamese: <b>vi-vn</b></li> </ul> <p>The locale tag is case sensitive.</p> <p>You can use the preferredLanguage tag to specify the locale if displayName, nativeName, and Name are in multibytes. If the locale tag is present in the xml, locale tag is preferred over the preferredLanguage tag.</p> | Optional           |                        |
| Name                                                | This is a Native Name Data field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Mandatory          | Max length 27          |
| Enable Reachability for Domain Control SIP Stations | The system enables Reachability on SIP endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Optional           |                        |

*Table continues...*

| Attribute | Attribute Description | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                 |
|-----------|-----------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                       |                    | <p>If you select <b>Calculate Route Pattern</b> check box, the system:</p> <ul style="list-style-type: none"> <li>• Populates the <b>Sip Trunk</b> field</li> <li>• Makes <b>Sip Trunk</b> field read-only.</li> </ul> |
|           |                       | Optional           |                                                                                                                                                                                                                        |

## Attribute details defined in the Messaging communication profile XSD

| Attribute                                  | Attribute Description                                                                                                                              | Mandatory/Optional | Validation Constraints                                                                                                   |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------|
| Messaging System Name<br>messagingName     | The name of Messaging System                                                                                                                       | Mandatory          |                                                                                                                          |
| Use Existing Mailbox number<br>useExisting | true if already created mailbox number is to be used. false if available mailbox number is to be used.                                             | Optional           |                                                                                                                          |
| Messaging Template<br>messagingTemplate    | Specifies the messaging template of a subscriber.                                                                                                  | Optional           |                                                                                                                          |
| Password<br>password                       | Specifies the default password the subscriber must use to log in to his or her mailbox.                                                            | Mandatory          | The password must be from 3 to 15 digits and adhere to system policies that you set on the Avaya Aura® Messaging server. |
| deleteOnUnassign                           |                                                                                                                                                    | Optional           |                                                                                                                          |
| Class of service<br>cos                    | The class of service for this subscriber. The COS controls subscriber access to many features and provides general settings, such as mailbox size. | Optional           | Valid ranges from 0 to 995                                                                                               |

*Table continues...*

| Attribute                   | Attribute Description                                                                                                                                                                                                                                                                                                               | Mandatory/Optional | Validation Constraints                                  |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------|
| Community ID<br>communityID | Specifies the default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers.                                                                                                                                                                                 | Optional           | The default value is 1.                                 |
| Email Handle<br>emailHandle | Specifies the name that appears before the machine name and domain in the subscriber's e-mail address. The machine name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.                                                                                                 | Optional           |                                                         |
| Common Name<br>commonName   | Specifies the display name of the subscriber in address book listings, such as those for e-mail client applications.                                                                                                                                                                                                                | Optional           | The name you enter can be 1 to 64 characters in length. |
| secondaryExtension          | Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers. | Optional           | Valid values 0 to 9<br>number values of length 10       |

*Table continues...*



| Attribute             | Attribute Description                                                                                                                                                                            | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Zone<br>timezone | This is the time zone for Avaya Aura® Messaging time subscribers.                                                                                                                                | Optional           | <p>Time zone in the StandardizedName format. For example, America/Phoenix.</p> <p>The field applies to Avaya Aura® Messaging 6.3 and later only.</p> <p> <b>Note:</b></p> <p>If the value is not in the standardized name format, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.</p> |
| mmSpecific            | This is complex type for Messaging Messaging specific fields data.                                                                                                                               | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| numericAddress        | <p>This is field of Messaging specific data.</p> <p>Specifies a unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.</p> | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| pbxExtension          | <p>This is field of Messaging specific data.</p> <p>The primary telephone extension of the subscriber.</p>                                                                                       | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| telephoneNumber       | <p>This is field of Messaging specific data.</p> <p>The telephone number of the subscriber as displayed in address book listings and client applications.</p>                                    | Optional           | <p>The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses (()) and ()).</p>                                                                                                                                                                                                                               |

Table continues...

| Attribute                | Attribute Description                                                                                                                                                                                                                                                                            | Mandatory/Optional | Validation Constraints                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| asciiVersionOfName       | This is field of Messaging specific data.<br><br>If the subscriber name is entered in multibyte character format, then this field specifies the ASCII translation of the subscriber name.                                                                                                        | Optional           |                                                                                                                                                                                   |
| expirePassword           | This is field of Messaging specific data.<br><br>Specifies whether your password expires or not.                                                                                                                                                                                                 | Optional           | You can choose one of the following: <ul style="list-style-type: none"> <li>• yes: for password to expire</li> <li>• no: if you do not want your password to expire</li> </ul>    |
| mailBoxLocked            | This is field of Messaging specific data.<br><br>Specifies whether you want your mailbox to be locked. A subscriber mailbox can become locked after two unsuccessful login attempts.                                                                                                             | Optional           | You can choose one of the following: <ul style="list-style-type: none"> <li>• no: to unlock your mailbox</li> <li>• yes: to lock your mailbox and prevent access to it</li> </ul> |
| personalOperatorMailbox  | This is field of Messaging specific data.<br><br>Specifies the mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting. | Optional           |                                                                                                                                                                                   |
| personalOperatorSchedule | This is field of Messaging specific data.<br><br>Specifies when to route calls to the backup operator mailbox. The default value for this field is Always Active.                                                                                                                                | Optional           |                                                                                                                                                                                   |

Table continues...

| Attribute       | Attribute Description                                                                                                         | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tuiMessageOrder | <p>This is field of Messaging specific data.</p> <p>Specifies the order in which the subscriber hears the voice messages.</p> | Optional           | <p>You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• urgent first then newest: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• oldest messages first: to direct the system to play messages in the order they were received.</li> <li>• urgent first then oldest: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</li> <li>• newest messages first: to direct the system to play messages in the reverse order of how they were received.</li> </ul> |

*Table continues...*

| Attribute        | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| intercomPaging   | <p>This is field of Messaging specific data.</p> <p>Specifies the intercom paging settings for a subscriber.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          | Optional           | <p>You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• paging is off: to disable intercom paging for this subscriber.</li> <li>• paging is manual: if the subscriber can modify, with Subscriber Options or the TUI, the setting that allows callers to page the subscriber.</li> <li>• paging is automatic: if the TUI automatically allows callers to page the subscriber.</li> </ul> |
| voiceMailEnabled | <p>This is field of Messaging specific data.</p> <p>Specifies whether a subscriber can receive messages, email messages and callanswer messages from other subscribers. You can choose one of the following: - yes: to allow the subscriber to create, forward, and receive messages. - no: to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.</p> | Optional           |                                                                                                                                                                                                                                                                                                                                                                                                                       |

*Table continues...*

| Attribute      | Attribute Description                                                                                                                                                                             | Mandatory/Optional | Validation Constraints |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| miscellaneous1 | This is field of Messaging specific data.<br><br>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |                    | Max length 51          |
| miscellaneous2 | This is field of Messaging specific data.<br><br>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |                    | Max length 51          |
| miscellaneous3 | This is field of Messaging specific data.<br><br>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |                    | Max length 51          |
| miscellaneous4 | This is field of Messaging specific data.<br><br>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |                    | Max length 51          |

*Table continues...*

| Attribute         | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                  | Mandatory/Optional | Validation Constraints                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cmmSpecific       | <p>This is field of Messaging specific data.</p> <p>Specifies the number of the switch on which this subscriber's extension is administered.</p>                                                                                                                                                                                                                                                                                       | Optional           | <p>You can enter "0" through "99", or leave this field blank.</p> <ul style="list-style-type: none"> <li>• Leave this field blank if the host switch number should be used.</li> <li>• Enter a "0" if no message waiting indicators should be sent for this subscriber. You should enter 0 when the subscriber does not have a phone on any switch in the network.</li> </ul> |
| accountCode       | <p>This is field of Communication Manager Messaging data.</p> <p>Specifies the Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.</p> | Optional           |                                                                                                                                                                                                                                                                                                                                                                               |
| coveringExtension | <p>This is field of Communication Manager Messaging data.</p> <p>Specifies the number to be used as the default destination for the Transfer Out of Messaging feature.</p>                                                                                                                                                                                                                                                             | Optional           | <p>You can enter 3 to 10 digits in this field depending on the length of the system's extension, or leave this field blank.</p>                                                                                                                                                                                                                                               |

*Table continues...*

| Attribute      | Attribute Description                                                                                                                                                                                                 | Mandatory/Optional | Validation Constraints |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| miscellaneous1 | <p>This is field of Communication Manager Messaging data.</p> <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> | Optional           | Max length 11          |
| Miscellaneous2 | <p>This is field of Communication Manager Messaging data.</p> <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> | Optional           | Max length 11          |
| Miscellaneous2 | <p>This is field of Communication Manager Messaging data.</p> <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> | Optional           | Max length 11          |
| Miscellaneous4 | <p>This is field of Communication Manager Messaging data.</p> <p>Specifies additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system.</p> | Optional           | Max length 11          |

## Attribute details defined in the Session Manager communication profile XSD

| Attribute                                | Attribute Description                                                                                                                                                                                                                                                                              | Mandatory/Optional | Validation Constraints |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| Primary Session Manager<br>primarySM     | The name of the Session Manager instance that must be used as the home server for a communication profile. As a home server, the primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura® network. | Mandatory          | -                      |
| Secondary Session Manager<br>secondarySM | If a secondary Session Manager instance is specified, this Session Manager provides continued service to SIP devices associated with this communication profile when the primary Session Manager is unavailable.                                                                                   | Optional           | -                      |

*Table continues...*



| Attribute                                   | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Mandatory/Optional | Validation Constraints |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| Survivability Server<br>survivabilityServer | <p>For local survivability, you can specify the name of a survivability server, a SIP entity, to provide survivability communication services for devices associated with a communication profile if the local connectivity to Session Manager instances in the Aura Core is lost.</p> <p>If you specify a Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to the Communication Manager remote survivability server resident with the Branch Session Manager.</p> <p> <b>Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, the Communication Manager associated with the application must be the main Communication Manager for the Communication Manager remote survivability server resident with</p> | Optional           | -                      |

Table continues...

| Attribute                                                                                     | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Mandatory/Optional | Validation Constraints |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
|                                                                                               | Branch Session Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                    |                        |
| Max. Simultaneous Devices<br>maxSimultaneousDevices                                           | The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                             |                    |                        |
| Block New Registration When Maximum Registrations Active<br>blockNewRegistrationWhenMaxActive | <p>Set the value to true or false. If you do not set the attribute, by default, the system sets the attribute to false.</p> <p>If you set to true and if an endpoint tries to register using this communication profile when the maximum number of allowed simultaneous registrations reaches, the endpoint cannot register with Session Manager. The endpoint does not have the SIP service.</p> <p>If the value is set to false, the default, the endpoint can register only after the system cancels the registration of the oldest endpoint. The stopped endpoint does not have the SIP service.</p> |                    |                        |

*Table continues...*

| Attribute                                                  | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                | Mandatory/Optional | Validation Constraints |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| Origination Application Sequence<br>originationAppSequence | <p>An Application Sequence that is invoked when calls are routed from this user.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> | Optional           | -                      |
| Termination Application Sequence<br>terminationAppSequence | <p>An Application Sequence that is invoked when calls are routed to this user.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> | Optional           | -                      |

Table continues...

| Attribute                                | Attribute Description                                                                                                                                                                                                                                                                                                                                                                             | Mandatory/Optional | Validation Constraints |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------|
| Home Location<br>homeLocation            | The home location that you set from <b>Routing &gt; Locations</b> to support mobility for a user. When this user calls numbers that are not associated with an administered user, dial-plan rules that are set in <b>Routing &gt; Dial Patterns</b> will be applied to complete the call based on this home location regardless of the physical location of the SIP device used to make the call. | Mandatory          | -                      |
| Conference Factory Set<br>confFactorySet | The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.<br><br>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.                                                                                                                                      | Optional           | -                      |

## Attribute details defined in the Avaya Aura® Conferencing profile XSD

| Attribute                                 | Attribute Description                                                                                                                                                                                                                                                                                                                                                                                       | Mandatory/Optional                                             | Validation Constraints |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|------------------------|
| User Template<br>template                 | Specify the name of the User Template. User Templates are created in Avaya Aura Conferencing Provisioning Client. The following default templates always exist:<br><br>executive,<br>desktop_user_with_video,<br>desktop_user_no_video,<br>desktop_user_low_priority, guest_user_no_video,<br>event_1000,<br>event_2000,<br>event_3000.                                                                     | Mandatory                                                      | -                      |
| Location<br>location                      | Specify location for the user.<br><br>Location is a mandatory field. However, Conferencing can get the value of location from the <b>Location</b> field in Conferencing Profile.<br><br>Conferencing can also get the value of location from the <b>Home Location</b> field in Session Manager Profile if Session Manager profile is configured and the location in Conferencing Profile is not configured. | Mandatory                                                      | -                      |
| Participant Security Code<br>securityCode | The participant code for the chairperson bridge.                                                                                                                                                                                                                                                                                                                                                            | Mandatory if the autoGeneratedCodeLength parameter is not set. | -                      |
| Moderator Security Code<br>moderatorPin   | The unique participant code that you use to login to a conference as a moderator.                                                                                                                                                                                                                                                                                                                           | Mandatory if the autoGeneratedCodeLength parameter is not set. | -                      |

*Table continues...*

| Attribute                                                                                 | Attribute Description                                                                                                                                                                                                                                                                                                                       | Mandatory/Optional                                          | Validation Constraints                     |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|--------------------------------------------|
| Auto Generated Participant and Moderator Security Codes Length<br>autoGeneratedCodeLength | This parameter shows that Participant and Moderator Security Codes must be auto-generated and must specify the length of such auto-generated codes.                                                                                                                                                                                         | Optional                                                    | The value can be integers between 6 and 8. |
| Presenter Security Code<br>eventConfCode                                                  | Specify Presenter Security Code.<br><br>In an Event Conference, when you enter the Presenter Security Code, the system assigns you the presenter role. Event Conference Host sets the Presenter Security Code. Presenter Security Code is mandatory if User Template contains Conferencing Class Of Service, supporting event conferencing. | Mandatory if the User Template supports event conferencing. | -                                          |

## Import Users field descriptions

Use this page to bulk import users and their attributes from a valid XML or Excel file.

### File Selection

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Import File Type</b> | The type of the file from where you import the users. The options are: <ul style="list-style-type: none"> <li>• XML</li> <li>• Excel</li> </ul>                                                                                                                                                                                                                                     |
| <b>Select File</b>             | The path and name of the XML or Excel file from which you import the users.<br><br>If you select the Excel file option, use the template that System Manager supports. You can download the template from <b>User Management &gt; Manage Users &gt; More Actions &gt; Download Excel Template</b> .<br><br>If a file type does not match, System Manager displays an error message. |
| Button                         | Description                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Browse</b>                  | Displays a dialog box to select the file from which you import the users.                                                                                                                                                                                                                                                                                                           |

## General

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Error Configuration</b>          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Abort on first error:</b> Aborts importing the user records when the import user operation encounters the first error in the import file containing the user records.</li> <li>• <b>Continue processing other records:</b> Imports the next user record even if the import user operation encounters an error while importing a user record.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Select Import Type</b>                  | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Complete:</b> Imports users with all the user attributes.</li> <li>• <b>Partial:</b> Imports users with specific user attributes.</li> </ul> <p><b>Select Import Type</b> is available only for imports using the XML file.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Skip:</b> Skips a matching user record that already exists in the system during an import operation. Currently, with this option you can add a new communication profile to a communication profile set but you cannot update an existing communication profile in a communication profile set.</li> </ul> <p> <b>Note:</b></p> <p>This option is not available if you select the <b>Partial</b> option in <b>Select Import Type</b>.</p> <ul style="list-style-type: none"> <li>• <b>Replace:</b> Re-imports or replaces all the data for a user including access control lists, contact lists, and so on. With this option, you can replace a user and the associated data of the user.</li> </ul> <p> <b>Note:</b></p> <p><b>Replace</b> is available only for imports using the XML file.</p> <ul style="list-style-type: none"> <li>• <b>Merge:</b> Imports the user data at an even greater degree of granularity. Using this option you can simultaneously perform both add and update operation of users. For example, add a contact to a contact list and update a last name.</li> <li>• <b>Delete:</b> Deletes the user records from the database that match the records in the input file.</li> </ul> <p> <b>Note:</b></p> <p>The system confirms that a user already exists in the database by matching the login name of the user in the database with the login name of the user in the imported file.</p> |

## Job Schedule

| Name                | Description                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Job</b> | The options for configuring the schedule of the job: <ul style="list-style-type: none"> <li>• <b>Run immediately:</b> Use this option to run the import job immediately.</li> <li>• <b>Schedule later:</b> Use this option to run the job at the specified date and time.</li> </ul> |
| <b>Date</b>         | The date on which you run the import users job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.                                                         |
| <b>Time</b>         | The time of running the import users job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.                                                                     |
| <b>Time Zone</b>    | The time zone of your region.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.                                                                                                                                                  |

| Button        | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| <b>Import</b> | Imports or schedules the import operation based on the option you selected. |

## Manage Job

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b> | Use this check box to select a job.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Scheduled Time</b>   | The time and date of scheduling the job.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Status</b>           | The current status of the job. The following are the different status of a job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is completed.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. PARTIAL FAILURE: The job execution has partially failed.</li> <li>6. FAILED: The job execution has failed.</li> </ol> |
| <b>Job Name</b>         | A link to the Scheduler user interface. You can also cancel the job from the Scheduler user interface.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>% Complete</b>       | The job completion status in percentage.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>User Records</b>     | The total user records in the input file.                                                                                                                                                                                                                                                                                                                                                                                                                                   |

*Table continues...*



| Name            | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Warnings</b> | The number of user records in the input file with warnings.         |
| <b>Errors</b>   | The number of user records in the input file that failed to import. |

| Button              | Description                                                                                                                                                                                |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Job</b>     | Displays the details of the selected job.                                                                                                                                                  |
| <b>Cancel Job</b>   | Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.                                                                          |
| <b>Delete Job</b>   | Deletes the selected job.                                                                                                                                                                  |
| <b>Refresh</b>      | Refreshes the job information in the table.                                                                                                                                                |
| <b>Show</b>         | Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select <b>All</b> to view all the jobs on a single page. |
| <b>Select: All</b>  | Selects all the jobs in the table.                                                                                                                                                         |
| <b>Select: None</b> | Clears the check box selections.                                                                                                                                                           |
| <b>Previous</b>     | Displays jobs in the previous page.                                                                                                                                                        |
| <b>Next</b>         | Displays jobs in the next page.                                                                                                                                                            |
| <b>Done</b>         | Navigates to the <b>User Management</b> page.                                                                                                                                              |

## Import Users – Job Details field descriptions

The Import Users-Job Details page displays the details of the selected job.

| Name                       | Description                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                | The import job that the end user initiates.                                                                                                                                                              |
| <b>Scheduled by</b>        | The name of the user who initiates or schedules the import job                                                                                                                                           |
| <b>Scheduled at</b>        | The start time of the import job.                                                                                                                                                                        |
| <b>Error Configuration</b> | The value that was configured for error while scheduling the Import Job. The values are <b>Abort on first error</b> and <b>Continue processing other records</b> .                                       |
| <b>Import Type</b>         | The value configured for the <b>Import Type</b> field while scheduling the import job. The values are <b>Complete</b> and <b>Partial</b> .                                                               |
| <b>Import Option</b>       | The value that was configured for the <b>If a matching record already exists</b> field while scheduling the import job. The values are <b>Skip</b> , <b>Merge</b> , <b>Replace</b> , and <b>Delete</b> . |
| <b>End</b>                 | The end date and time of the job.                                                                                                                                                                        |
| <b>Status</b>              | The status of the job.                                                                                                                                                                                   |
| <b>File</b>                | The name of the file that is used to import the user records.                                                                                                                                            |
| <b>Count</b>               | The total number of user records in the input file.                                                                                                                                                      |
| <b>Success</b>             | The total number of user records that are successfully imported.                                                                                                                                         |

*Table continues...*

| Name             | Description                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Fail</b>      | The total number of user records that failed to import.                                                                  |
| <b>Warning</b>   | The total number of user records that successfully imported, however, there are warnings generated for the user records. |
| <b>Message</b>   | A message that indicates whether the import is successful or failure.                                                    |
| <b>Completed</b> | The percentage completion of the import.                                                                                 |

| Name                 | Description                                                   |
|----------------------|---------------------------------------------------------------|
| <b>Line Number</b>   | The line number in the file where the error occurred.         |
| <b>Login Name</b>    | The login name of the user record that failed to be imported. |
| <b>Error Message</b> | A brief description of the error.                             |

| Button          | Description                                                                                                                                                                                                                                                                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Download</b> | Exports and saves the user import error records in an XML file to the specified destination.<br><br> <b>Note:</b><br>This button is not available if there are no error records for user Import Jobs or if the import job type is set to <b>Abort on first error</b> . |
| <b>Cancel</b>   | Returns to the Import Users page.                                                                                                                                                                                                                                                                                                                       |

To enable the **Download** button, on the User bulk import configuration page, set the **Enable Error File Generation** attribute to **True**.

To navigate to the User bulk import configuration page from the System Manager console, click **Services > Configurations > Settings > SMGR > User BulkImport profile**.

## Import Global Settings field descriptions

Use this page to bulk import shared addresses, public contacts, and presence access control list (ACLs) from a valid XML file. These imported items are also called global user settings.

### File Selection

| Name               | Description                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select File</b> | The path and name of the XML file from which you must import the global settings records.<br><br>If a file type does not match, System Manager displays an error message. |

| Button        | Description                                                                                |
|---------------|--------------------------------------------------------------------------------------------|
| <b>Browse</b> | Opens a dialog box to select the file from which you must import the global user settings. |

## General

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Error Configuration</b>          | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Abort on first error:</b> Stops importing the global user settings records when User Management encounters the first error in the import file containing the global user settings records.</li> <li>• <b>Continue processing other records:</b> Imports the next global user settings record even if User Management encounters an error while importing a global user settings record.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Skip:</b> Skips a matching global user settings record that already exists in the system database during an import operation. Currently, using this option you can add a new public contact to a public contact set but you cannot update an existing public contact in a public contact set.</li> <li>• <b>Merge:</b> Imports the global user settings data at an even greater degree of granularity. For example, add a shared address to a shared address list or update a public contact.</li> <li>• <b>Replace:</b> Re-imports or replaces all the global user setting records in the import file. This is essentially the ability to replace a user along with the other data related to the global user settings.</li> <li>• <b>Delete:</b> Deletes the global setting records from the database that matches the records in the input XML file.</li> </ul> |

## Job Schedule

| Name                | Description                                                                                                                                                                                                                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Job</b> | <p>The settings for configuring the schedule of the job:</p> <ul style="list-style-type: none"> <li>• <b>Run immediately:</b> Use this option to run the import job immediately.</li> <li>• <b>Schedule later:</b> Use this option to run the job at the specified date and time.</li> </ul> |
| <b>Date</b>         | <p>The date when you must run the import job. The date format is mm dd yyyy. You can use the calendar icon to choose a date.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                       |
| <b>Time</b>         | <p>The time of running the import job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                            |
| <b>Time Zone</b>    | <p>The time zone of your region.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                                                                                                   |

| Button        | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| <b>Import</b> | Imports or schedules the import operation based on the option you selected. |

## Manage Jobs

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b> | Use this check box to select a job.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Scheduled Time</b>   | The date and time when the job was scheduled.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Status</b>           | The current status of the job. The following are the different status of a job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is completed.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. PARTIAL FAILURE: The job execution has partially failed.</li> <li>6. FAILED: The job execution has failed.</li> </ol> |
| <b>Job Name</b>         | A link to the Scheduler user interface. You can also cancel the job from the Scheduler user interface.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>% Complete</b>       | The job completion status in percentage.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Records</b>          | The total number of global user settings records in the input file.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Error</b>            | The number of global user settings records in the input file that failed to import.                                                                                                                                                                                                                                                                                                                                                                                         |

| Button              | Description                                                                                                                                                                                |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Job</b>     | Shows the details of the selected job.                                                                                                                                                     |
| <b>Cancel Job</b>   | Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.                                                                          |
| <b>Delete Job</b>   | Deletes the selected job.                                                                                                                                                                  |
| <b>Refresh</b>      | Refreshes the job information in the table.                                                                                                                                                |
| <b>Show</b>         | Provides you an option to view all the jobs on the same page. If the table displaying scheduled jobs are spanning multiple pages, select <b>All</b> to view all the jobs on a single page. |
| <b>Select: All</b>  | Selects all the jobs in the table.                                                                                                                                                         |
| <b>Select: None</b> | Clears the check box selections.                                                                                                                                                           |
| <b>Previous</b>     | Displays jobs in the previous page.                                                                                                                                                        |
| <b>Next</b>         | Displays jobs in the next page.                                                                                                                                                            |
| <b>Done</b>         | Returns to the <b>User Management</b> page.                                                                                                                                                |
| <b>Cancel</b>       | Cancels the import operation and returns to the User Management page.                                                                                                                      |

## Job Details field descriptions

The Job Details page displays the details of the selected Job.

| Name                | Description                                                                  |
|---------------------|------------------------------------------------------------------------------|
| <b>Name</b>         | Specifies the name of the import job.                                        |
| <b>Scheduled by</b> | Name of the user who initiated or scheduled the import job.                  |
| <b>Scheduled at</b> | Start time of the scheduled job.                                             |
| <b>End</b>          | End date and time of the job.                                                |
| <b>Status</b>       | Status of the job.                                                           |
| <b>File</b>         | Name of the file that is used to import the global user settings records.    |
| <b>Count</b>        | Total number of global user settings records in the input file.              |
| <b>Success</b>      | Total number of global user settings records that are successfully imported. |
| <b>Fail</b>         | Total number of global user settings records that failed to import.          |
| <b>Message</b>      | The message that indicates whether the import is successful or failure.      |
| <b>Completed</b>    | Displays the percentage completion of the import.                            |

| Name                 | Description                               |
|----------------------|-------------------------------------------|
| <b>Record Number</b> | Failed XML element in the input XML file. |
| <b>Name</b>          | Name of the failed XML element.           |
| <b>Error Message</b> | A brief description of the error.         |

| Button        | Description                       |
|---------------|-----------------------------------|
| <b>Cancel</b> | Returns to the Import Users page. |

## Quick start to importing users

### Quick start to importing users

This section describes how to quickly create an XML file for importing users in bulk. This XML file includes user profiles with core attributes as well as with SIP phone (SIP communication profile).

### XML for user with core attributes

The table lists the minimal elements for mapping the user import XML with user interface fields.

**Table 3: Minimal elements**

| UI field                   | Description                                              | XML tag                                                                    | Possible value              |
|----------------------------|----------------------------------------------------------|----------------------------------------------------------------------------|-----------------------------|
| <b>Authentication Type</b> | Specifies the type of authentication.                    | <pre>&lt;authenticationType&gt; ... &lt;/authenticationType&gt; &gt;</pre> | Basic or Enterprise         |
| <b>First Name</b>          | Specifies the first name of the user.                    | <pre>&lt;givenName&gt; ... &lt;/givenName&gt;</pre>                        | First name of the user.     |
| <b>Login Name</b>          | Specifies the primary handle of user.                    | <pre>&lt;loginName&gt; ... &lt;/loginName&gt;</pre>                        | User log-in name.           |
| <b>Last Name</b>           | Specifies the last name of the user.                     | <pre>&lt;surname&gt; ... &lt;/surname&gt;</pre>                            | Last name of the user.      |
| <b>Login Password</b>      | Specifies the password used to log in to System Manager. | <pre>&lt;userPassword&gt; ... &lt;/userPassword&gt;</pre>                  | Login password of the user. |

### Sample XML with a single user profile

The following sample XML contains a user profile with basic fields. To create your own XML, replace the value of the tags explained in the Minimal elements table in *XML for user with core attributes*.

```
<?xml version="1.0" encoding="UTF-8"?>
 <!-- Root Element 'Users' represent collection of user (containing 1 or more users)-->
 <tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd" >

 <tns:user>
 <authenticationType>Basic</authenticationType>
 <givenName>John</givenName>
 <loginName>jmiller@avaya.com</loginName>
 <surname>Miller</surname>
 <userPassword>mypassword</userPassword>
 </tns:user>
 </tns:users>
```

The highlighted XML tag in the user profile XML represents the data for a single user tag that starts and ends with `</tns:user>`. To create multiple users in the same XML, repeat the highlighted content multiple times with different user values.

For example, the following sample XML contains two users, John Miller and Roger Philip. Note that there are two instances of the `<tns:user>` tag, one for each user.

```
<?xml version="1.0" encoding="UTF-8"?>
 <!-- Root Element 'Users' represent collection of user (containing 1 or more
```

```

users)-->
<tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >

 <tns:user>
 <authentication>TypeBasic</authenticationType>
 <givenName>John</givenName>
 <loginName>jmiller@avaya.com</loginName>
 <surname>Miller</surname>
 <userPassword>mypassword</userPassword>
 </tns:user>

 <tns:user>
 <authenticationType>Basic</authenticationType>
 <givenName>Roger</givenName>
 <loginName>rphilip@avaya.com</loginName>
 <surname>Philip</surname>
 <userPassword>mypassword</userPassword>
 </tns:user>

</tns:users>

```

 **Note:**

The XML is a text file. Therefore, you can edit this XML in any text editor.

## Related links

[XML for user with core attributes](#) on page 587

## Bulk import XML for users with SIP phone

To create a user XML, first perform the procedure for bulk importing users in the *Bulk importing users* section. If communication address is added to the user, then the **commPassword** field is mandatory.

To assign communication address, the mapping of Communication Profile for a new SIP user is as follows:

**Table 4: Mapping of Communication Profile for a new SIP user**

| UI field       | Description                                      | XML tag                                                                 | Possible value                                 |
|----------------|--------------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------|
| <b>Name</b>    | Specifies the name of the communication profile. | <pre> &lt;commProfileSetName&gt; ... &lt;/commProfileSetName&gt; </pre> | The unique name of this communication profile. |
| <b>Default</b> | Indicates whether this is a default profile.     | <pre> &lt;isPrimary&gt; ... &lt;/isPrimary&gt; </pre>                   | True or False.                                 |

The attributes to set up the communication address for a user are as follows:

**Table 5: User attributes to set up communication address**

| UI field       | Description                                              | XML tag                                                     | Possible value                                                  |
|----------------|----------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------|
| <b>Handle</b>  | Specifies the extension number of the user.              | <pre>&lt;handleName&gt; ... &lt;/handleName&gt;</pre>       | Extension number.                                               |
| <b>Type</b>    | Specifies the communication type of the user profile.    | <pre>&lt;handleType&gt; ... &lt;/handleType&gt;</pre>       | Communication type. For example, sip and smtp.                  |
| <b>SubType</b> | Specifies the communication subtype of the user profile. | <pre>&lt;handleSubType&gt; ... &lt;/handleSubType&gt;</pre> | Communication sub type. For example, username, e164, and msrtc. |
| <b>Domain</b>  | Specifies the domain name of the user.                   | <pre>&lt;domainName&gt; ... &lt;/domainName&gt;</pre>       | Name of the configured SIP domain name.                         |

The following is the mapping of Session Manager Communication profile elements with the corresponding user interface fields.

**Table 6: Mapping of Session Manager Communication Profile elements**

| UI field                                          | Description                                                                                                             | XML tag                                                                                                      | Possible value                     |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------|
| <b>Primary Session Manager</b>                    | Specifies the name of the primary Session Manager instance that is used as the home server for a communication profile. | <pre>&lt;sm:primarySM&gt; ... &lt;/sm:primarySM&gt;</pre>                                                    | Enter the name of Session Manager. |
| <b>Origination Application Sequence</b>           | Specifies the Application Sequence that is invoked when calls are routed from this user.                                | <pre>&lt;sm:originationAppSequence&gt; ... &lt;/sm:originationAppSequence&gt;</pre>                          | True or False.                     |
| <b>Termination Application Sequence</b>           | Specifies the Application Sequence that is invoked when calls are routed to this user.                                  | <pre>&lt;sm:terminationAppSequence&gt; ... &lt;/sm:terminationAppSequence&gt;</pre>                          |                                    |
| <b>Emergency Origination Application Sequence</b> | Specifies the emergency application sequence that is invoked when calls are routed from this user.                      | <pre>&lt;ns6:emergencyOriginationAppSequence&gt;app edpseq&lt;/ns6:emergencyOriginationAppSequence&gt;</pre> |                                    |

*Table continues...*



| UI field                                          | Description                                                                                      | XML tag                                                                                                                 | Possible value |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|----------------|
| <b>Emergency Termination Application Sequence</b> | Specifies the emergency application sequence that is invoked when calls are routed to this user. | <code>&lt;ns6:emergencyTerminationAppSequence&gt;app<br/>edpseq&lt;/<br/>ns6:emergencyTerminationAppSequence&gt;</code> |                |
| <b>Home Location</b>                              | Specifies the routing home location.                                                             | <code>&lt;sm:homeLocation&gt;<br/>...<br/>&lt;/sm:homeLocation&gt;</code>                                               |                |

The following is the mapping of CM Endpoint Profile elements with the corresponding user interface fields.

**Table 7: Mapping of CM Endpoint Profile elements**

| UI field            | Description                                                          | XML tag                                                                                     | Possible value                                |
|---------------------|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------|
| <b>System</b>       | Specifies the SIP Entity of the Communication Manager.               | <code>&lt;ipt:cmName&gt;<br/>...<br/>&lt;/ipt:cmName&gt;</code>                             | Name of the configured Communication Manager. |
| <b>Use Existing</b> | Indicates whether the station is already defined in the system.      | <code>&lt;ipt:useExistingExtension&gt;<br/>...<br/>&lt;/ipt:useExistingExtension&gt;</code> | True or False.                                |
| <b>Extension</b>    | Specifies the extension number for this profile.                     | <code>&lt;ipt:extension&gt;<br/>...<br/>&lt;/ipt:extension&gt;</code>                       |                                               |
| <b>Template</b>     | Specifies the template name used for creating the station.           | <code>&lt;ipt:template&gt;<br/>...<br/>&lt;/ipt:template&gt;</code>                         |                                               |
| <b>Set Type</b>     | Specifies the set type of the station.                               | <code>&lt;ipt:setType&gt;<br/>...<br/>&lt;/ipt:setType&gt;</code>                           |                                               |
| <b>Port</b>         | Specifies the port number from the list for the template you select. | <code>&lt;ipt:port&gt;<br/>...<br/>&lt;/ipt:port&gt;</code>                                 |                                               |

#### Related links

[Bulk importing of users](#) on page 379

## Sample XML file for a user with SIP Communication Profile

Here is the sample XML of a user profile with basic fields. To create your own XML, replace the value of the tags explained in the Mapping of CM Endpoint Profile elements table in *Bulk import XML for users with SIP phone*.

```
<?xml version="1.0" encoding="UTF-8"?>
 <!-- Root Element 'Users' represent collection of user (containing 1 or more
users)--
tns:users xmlns:tns="http://xml.avaya.com/schema/import" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xsi:schemaLocation="http://xml.avaya.com/schema/import
userimport.xsd" >
 <tns:user>
 <authenticationType>BASIC</authenticationType>
 <givenName>John</givenName>
 <loginName>jmiller@avaya.com</loginName>
 <surname>Miller</surname>
 <userPassword>mypassword</userPassword>
 <commPassword>12345</commPassword>
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 <handleList>
 <handle>
 <handleName>sip:jmiller@avaya.com</handleName>
 <handleType>sip</handleType>
 <handleSubType>msrtc</handleSubType>
 </handle>
 </handleList>
 <!--The below is extended communication profile-->
 <commProfileList>
 <commProfile xsi:type="sm:SessionManagerCommProfXML" xmlns:sm="http://
xml.avaya.com/schema/import_sessionmanager">
 <commProfileType>SessionManager</commProfileType>
 <sm:primarySM>IBM1-Performance</sm:primarySM>
 <sm:terminationAppSequence>Perf_CM_Appl_Seq</sm:terminationAppSequence>
 <sm:originationAppSequence>Perf_CM_Appl_Seq</sm:originationAppSequence>
 <sm:homeLocation>SIT Lab</sm:homeLocation>
 </commProfile>

 <commProfile xsi:type="ipt:xmlStationProfile" xmlns:ipt="http://xml.avaya.com/
schema/import_csm_cm">
 <CommProfileType>CM</commProfileType>
 <ipt:cmName>Performance_CM</ipt:cmName>
 <ipt:useExistingExtension>false</ipt:useExistingExtension>
 <ipt:extension>28000</ipt:extension>
 <ipt:template>DEFAULT_9620SIP_CM_5_2</ipt:template>
 <ipt:setType>9620SIP</ipt:setType>
 <ipt:port>S08012</ipt:port>
 </commProfile>
 </commProfileList>
 </commProfileSet>
 </tns:user>
</tns:users>
```

### Related links

[Bulk import XML for users with SIP phone](#) on page 589

---

# Managing public contacts

---

## Manage public contact list

An administrator defines public contacts for the users in System Manager. You can share the public contacts with all the users in System Manager.

A user with administrator permission can add, modify, and delete a public contact. While creating a public contact, you need to specify the details of contact that also includes the postal address and communication address of the public contact.

The public contacts defined in the system are the default public contacts for the users and access control list.

---

## Adding a new public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, click **New**.
3. On the New Public Contact page, in the **Contact Details** area, enter the appropriate information in the respective fields.

Enter valid information in these fields to successfully create a new public contact.

The localized display name must be a unique name. If you do not enter any information in the **Localized Display Name** field, the system automatically generates a localized display name for the public contact.

4. In the **Postal Address** area, click **New** to add postal address of the contact.
5. In the **Contact Address** area, click **New** to add contact address.

A contact address can be a phone number or any communication address that is supported by the application.

6. Click **Commit** to create a new public contact.

### Related links

[New Public Contact field descriptions](#) on page 601

---

## Modifying details of a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, click **Edit**.
3. On the Edit Public Contact page, modify the information of the contact.
4. Click **Commit**.

 **Note:**

Before you click **Commit**, ensure that you entered valid information in the mandatory fields.

### Related links

[Edit Public Contact field descriptions](#) on page 599

---

## Deleting public contacts

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, select one or more contacts.
3. Click **Delete**.
4. On the Contact Delete Confirmation page, click **Delete**.

The system deletes the contact from the default contact list of the user if the public contact is associated with the user.

---

## Viewing the details of a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, select a public contact and click **View**.

The View Public Contact page displays the details of a public contact.

### Related links

[View Public Contact field descriptions](#) on page 597

---

## Adding a postal address for a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, perform one of the following steps:
  - To add a postal address to a new public contact, click **New**.
  - To add a postal address to an existing public contact, select a public contact and click **Edit**.
3. Click **New** in the **Postal Address** area.
4. On the Add Address page, enter the appropriate information in the respective fields.  
Enter a valid information in these fields.
5. Click **Add** to create a new postal address for the public contact.
6. On the New Public Contact or Edit Public Contact page, click **Commit**.

### Related links

[Add Address field descriptions](#) on page 256

---

## Modifying postal address of a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.
3. On the Edit Public Contact page, select an address from the Postal Address section.
4. Click **Edit**.
5. On the Edit Address page, modify the information in the respective fields.  
The fields marked with an asterisk are mandatory. You must enter valid information in these fields.
6. Click **Add** to save the modified address.

### Related links

[Add Address field descriptions](#) on page 256

---

## Deleting the postal addresses of a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.
3. Select an address from the table in the Postal Address section, and click **Delete**.
4. Click **Commit** to save the changes.

---

## Choosing a shared address for a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. Click **Choose Shared Address**.
3. On the Choose Address page, select one or more shared addresses.
4. Click **Select** to add the selected addresses for the public contact.
5. Click **Commit**.

---

## Adding a contact address of a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. Click **New** in the **Contact Address** area.
3. On the Add Address page, enter the appropriate information in the respective fields.  
Enter a valid information in these fields.
4. Click **Add** to create a new contact address for the public contact.
5. On the New Public Contact page, click **Commit**.

### Related links

[Add Address field descriptions](#) on page 290

---

## Modifying the details of a public contact

### About this task

You can use this feature to modify the contact details, postal address, and contact address of an existing public contact.

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.
3. On the Edit Public Contact page, modify the information in the Contact Details, Postal Address, and Contact Address sections.

In the Postal Address and Contact Address section you can add, modify, and delete addresses in the respective sections.

The fields marked with an asterisk are mandatory. You must enter a valid information in these fields.

4. Click **Commit**.

### Related links

[Edit Address field descriptions](#) on page 291

---

## Deleting the contact address of a public contact

### Procedure

1. On the System Manager web console, click **Users > User Management > Public Contacts**.
2. On the Public Contacts page, select a public contact and click **Edit**.  
If you are on the New Public Contact page, follow Step 4.
3. In the **Contact Address** area, select one or more addresses from the list and click **Delete**.
4. Click **Commit** to save the changes.

---

## View Public Contact field descriptions

### Contact Details

| Name      | Description                   |
|-----------|-------------------------------|
| Last Name | The last name of the contact. |

*Table continues...*

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p> <b>Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>• Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>• Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Middle Name</b>                    | The middle name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                    | Displays a brief description of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Company</b>                        | The name of contact's company.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Localized Display Name</b>         | The localized display name of a user. It is typically the localized full name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Endpoint Display Name</b>          | The endpoint display name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Language Preference</b>            | Displays a list of languages from which you set one language as the preferred language for the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Postal Address

| Name                | Description                                              |
|---------------------|----------------------------------------------------------|
| <b>Name</b>         | The name of the contact.                                 |
| <b>Address Type</b> | The mailing address type such as home or office address. |
| <b>Street</b>       | The name of the street.                                  |
| <b>City</b>         | The name of the city or town.                            |
| <b>Postal Code</b>  | The name of the contact's company.                       |
| <b>Province</b>     | The full name of the contact's province.                 |
| <b>Country</b>      | The name of the contact's country.                       |

## Contact Address

| Name           | Description                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b> | The address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact. |
| <b>Type</b>    | The type of communication medium for interacting with the user.                                                                 |

*Table continues...*



| Name                     | Description                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Category</b>          | The categorization of the address based on the location.                                                                                            |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                           |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language. |

#### Related links

[Viewing the details of a public contact](#) on page 594

## Edit Public Contact field descriptions

### Contact Details

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>                      | The last name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p> <b>Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>• Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>• Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Middle Name</b>                    | The middle name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                    | Displays a brief description about the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Company</b>                        | The name of contact's company.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Localized Display Name</b>         | The localized display name of a user. It is typically the localized full name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Endpoint Display Name</b>          | The endpoint display name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Language Preference</b>            | Displays a list of languages from which you set one language as the preferred language for the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Update Time</b>                    | The time when the contact information was last updated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Source</b>                         | The source for provisioning the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Postal Address

| Name                | Description                                              |
|---------------------|----------------------------------------------------------|
| <b>Name</b>         | The name of the contact.                                 |
| <b>Address Type</b> | The mailing address type such as home or office address. |
| <b>Street</b>       | The name of the street.                                  |
| <b>City</b>         | The name of the city or town.                            |
| <b>Postal Code</b>  | The name of the contact's company.                       |
| <b>Province</b>     | The full name of the contact's province.                 |
| <b>Country</b>      | The name of the contact's country.                       |

| Button                       | Description                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>                  | Displays the <b>Edit Address</b> page. Use this page to add a new postal address of the public contact.         |
| <b>New</b>                   | Displays the <b>Add Address</b> page. Use this page to modify an existing postal address of the public contact. |
| <b>Delete</b>                | Deletes the selected public contacts.                                                                           |
| <b>Choose Shared Address</b> | Displays the <b>Choose Address</b> page. Use this page to choose addresses of the public contact.               |

## Contact Address

| Name                     | Description                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | The address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.                     |
| <b>Type</b>              | The type of communication medium for interacting with the user.                                                                                     |
| <b>Category</b>          | The categorization of the address based on the location.                                                                                            |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                           |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language. |

| Button        | Description                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------|
| <b>Edit</b>   | Displays the <b>Edit Address</b> page. Use this page to edit a contact address of the public contact. |
| <b>New</b>    | Displays the <b>Add Address</b> page. Use this page to add a contact address of the public contact.   |
| <b>Delete</b> | Deletes the selected public contacts.                                                                 |

| Button        | Description                                     |
|---------------|-------------------------------------------------|
| <b>Commit</b> | Saves the modified information to the database. |

## Related links

[Modifying details of a public contact](#) on page 594

## New Public Contact field descriptions

### Contact Details

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>                      | The last name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Last Name (Latin Translation)</b>  | <p>The user-preferred last name that the system must display on the endpoints. For example, Miller.</p> <p>Typically, the name is in the written or spoken language of the user.</p> <p> <b>Note:</b></p> <p>When you create a user, if the <b>Last Name (Latin Translation)</b> and <b>First Name (Latin Translation)</b> fields are:</p> <ul style="list-style-type: none"> <li>• Blank, the system displays the last name and first name in the fields. The values change when the last and first names change.</li> <li>• Filled, the values remain the same even after you change the values in the <b>Last Name</b> and <b>First Name</b> fields.</li> </ul> |
| <b>First Name</b>                     | The first name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>First Name (Latin Translation)</b> | <p>The user-preferred first name that the system must display on the endpoints. For example, John.</p> <p>Typically, the name is in the written or spoken language of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Middle Name</b>                    | The middle name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>                    | Displays a brief description of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Company</b>                        | The name of company.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Localized Display Name</b>         | The localized display name of a user. It is typically the localized full name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Endpoint Display Name</b>          | The endpoint display name of the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Language Preference</b>            | Displays a list of languages from which you set one language as the preferred language for the contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### Postal Address

| Name                | Description                                              |
|---------------------|----------------------------------------------------------|
| <b>Name</b>         | The name of the contact.                                 |
| <b>Address Type</b> | The mailing address type such as home or office address. |
| <b>Street</b>       | The name of the street.                                  |
| <b>City</b>         | The name of the city or town.                            |
| <b>Postal Code</b>  | The name of the contact's company.                       |
| <b>Province</b>     | The full name of the contact's province.                 |
| <b>Country</b>      | The name of the contact's country.                       |

| Button                       | Description                                                                                                     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>                  | Displays the <b>Edit Address</b> page. Use this page to add a new postal address of the public contact.         |
| <b>New</b>                   | Displays the <b>Add Address</b> page. Use this page to modify an existing postal address of the public contact. |
| <b>Delete</b>                | Deletes the selected public contacts.                                                                           |
| <b>Choose Shared Address</b> | Displays the <b>Choose Address</b> page. Use this page to choose addresses of the public contact.               |

## Contact Address

| Name                     | Description                                                                                                                                         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | The address that you can use to communicate with the contact. This can be a phone number, e-mail address, or IM of the contact.                     |
| <b>Type</b>              | The type of communication medium for interacting with the user.                                                                                     |
| <b>Category</b>          | The categorization of the address based on the location.                                                                                            |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                           |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language. |

| Button        | Description                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------|
| <b>Edit</b>   | Displays the <b>Edit Address</b> page. Use this page to edit a contact address of the public contact. |
| <b>New</b>    | Displays the <b>Add Address</b> page. Use this page to add a contact address of the public contact.   |
| <b>Delete</b> | Deletes the selected public contacts.                                                                 |

| Button        | Description                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | <p>Creates a new contact.</p> <p> <b>Note:</b></p> <p>Enter valid information in the mandatory fields to successfully create a new contact.</p> |

## Related links

[Adding a new public contact](#) on page 593

## Public Contacts field descriptions

Use this page to add new public contacts, and modify and delete the existing contacts.

## Public Contacts

| Name                   | Description                             |
|------------------------|-----------------------------------------|
| <b>Last Name</b>       | The last name of the public contact.    |
| <b>First Name</b>      | The first name of the public contact.   |
| <b>Display Name</b>    | The display name of the public contact. |
| <b>Contact Address</b> | The address of the public contact.      |
| <b>Description</b>     | A brief description of the contact.     |

| Button                         | Description                                                                                                     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>View</b>                    | Displays the <b>View Public Contact</b> page. Use this page to view the details of the selected public contact. |
| <b>Edit</b>                    | Displays the <b>Edit Public Contact</b> page. Use this page to modify the information of the selected contact.  |
| <b>New</b>                     | Display the <b>New public Contact</b> page. Use this page to add a new public contact.                          |
| <b>Delete</b>                  | Deletes the selected contacts.                                                                                  |
| <b>Filter: Advanced Search</b> | Displays fields that you can use to specify the search criteria for searching a public contact.                 |
| <b>Filter: Disable</b>         | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                  |
| <b>Filter: Enable</b>          | Displays text fields under the columns that you can use to set the filter criteria. This is a toggle button.    |
| <b>Filter: Apply</b>           | Filters contacts based on the filter criteria.                                                                  |

## Criteria section

The page displays the following fields when you click **Advanced Search** . You can find the **Advanced Search** link at the upper-right corner of the public contact table.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>Field 1– The list of criteria that you can use to search public contacts. The options are: <ol style="list-style-type: none"> <li>1. Last Name: Searches public contacts by last name.</li> <li>2. First Name: Searches public contacts by first name.</li> <li>3. Display Name: Searches public contacts by display name.</li> <li>4. Contact Address: Searches public contacts by contact address.</li> </ol> </li> <li>Field 2 – The operator for evaluating the expression. The list of operators displayed depends on the type of criterion that you selected in field 1.</li> <li>Field 3 – The search value for the search criterion selected in field 1.</li> </ul> |

---

## Managing shared addresses

---

### Manage shared address

Shared address contains common addresses that you can specify for one or more users in the enterprise. The user with appropriate permissions can create a new shared address and modify and delete an existing shared address. For example, you can add the address of the company in the list of shared address and other users can use this address as their alternative address.

---

### Assigning a shared address to the user

#### About this task

Use this procedure to choose a shared address for a user from the common addresses database. You can assign and remove a shared address.

#### Procedure

1. On the System Manager web console, click **Users > User Management > Manage Users**.
2. On the Manage Users page, do one of the following:
  - To assign shared addresses to a new user while creating the user, click **New**.
  - To assign shared addresses to an existing user, select the user, and click **Edit**.
3. On the User Profile | Add page or the User Profile | Edit | <User Name> page, click **Identity > Address > Choose Shared Address**.
4. On the Choose Shared Address page, click one or more shared addresses.

For a new user, enter valid information in all mandatory fields on all tabs of the User Profile | Add page before you click **Commit**. If you enter invalid information, the system displays an error message.

5. Click **Select**.
6. Click one of the following:
  - **Commit**: To save the changes.
  - **Commit & Continue**: To save the changes and stay on the same page for making further modifications.

#### Related links

[Choose Address field descriptions](#) on page 257

---

## Adding a shared address

### Procedure

1. On the System Manager web console, click **Users > User Management > Shared Addresses**.
2. On the Shared Address page, click **New**.
3. On the Add Address page, enter the appropriate information.
4. Click **Add**.

### Result

The new address is available as shared address and you can specify this address when you create or modify a user account.

---

## Modifying a shared address

### Procedure

1. On the System Manager web console, click **Users > User Management > Shared Addresses**.
2. On the Shared Address page, select an address and click **Edit**.
3. On the Edit Address page, modify the information in the fields.
4. Click **Add**.

---

## Deleting a shared address

### About this task

You can use this feature to delete a shared address. You cannot delete a shared address if the address is associated with one or more users.

### Procedure

1. On the System Manager web console, click **Users > User Management > Shared Addresses**.
2. On the Shared Address page, select the address you want to delete and click **Delete**.

---

## Add Address field descriptions

| Name                     | Description                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Address Name</b>      | The unique label that identifies the mailing address.                                                                            |
| <b>Address Type</b>      | The mailing address type such as home or office address.                                                                         |
| <b>Building</b>          | The name of the building.                                                                                                        |
| <b>Room</b>              | The number or name of the room.                                                                                                  |
| <b>Street</b>            | The name of the street.                                                                                                          |
| <b>City</b>              | The name of the city or town.                                                                                                    |
| <b>State or Province</b> | The full name of the province.                                                                                                   |
| <b>Postal Code</b>       | The postal code or zip code used by postal services to route mail to a destination. For the United States, specify the Zip code. |
| <b>Country</b>           | The name of the country.                                                                                                         |

### Phone Details section

| Name                        | Description                                                                    |
|-----------------------------|--------------------------------------------------------------------------------|
| <b>Business Phone</b>       | The business phone number of the user.                                         |
| <b>Other Business Phone</b> | The secondary or alternate business phone number if applicable.                |
| <b>Home Phone</b>           | The residential phone number of the user.                                      |
| <b>Other Home Phone</b>     | The secondary or alternate residential phone number if applicable.             |
| <b>Mobile Phone</b>         | The mobile number of the user.                                                 |
| <b>Other Mobile Phone</b>   | The secondary or alternate mobile number of the user if applicable.            |
| <b>Fax</b>                  | The telephone number for direct reception of faxes.                            |
| <b>Pager</b>                | The number used to make calls to the pager of the user.                        |
| <b>Other Pager</b>          | The secondary or alternate number used to make calls to the pager of the user. |

| Button        | Description                           |
|---------------|---------------------------------------|
| <b>Add</b>    | Adds the mailing address of the user. |
| <b>Cancel</b> | Cancels the add address operation.    |

### Related links

[Modifying a shared address](#) on page 605

[Adding a shared address](#) on page 605

---

## Edit Address field descriptions

Use this page to edit the details of a contact's communication address.



| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b>           | Displays the address that you can use to communicate with the contact. This can be a phone number, email address, SIP, or IM of the contact. The format of the address must conform to the type of address that you select in the <b>Type</b> field.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Type</b>              | Displays the type of address. The types of addresses are: <ul style="list-style-type: none"> <li>• <b>Phone</b>: This address type supports phone numbers.</li> <li>• <b>SIP</b>: This address type supports SIP-based communication.</li> <li>• <b>MSRTC</b>: This address type supports communication with a Microsoft RTC server.</li> <li>• <b>IBM Sametime</b>: This address type supports communication with IBM Sametime. Specify the address in the DN=IBMHandle format.</li> <li>• <b>XMPP</b>: This address type supports xmpp-based communication.</li> <li>• <b>SMTP</b>: This address type supports communication with the SMTP server.</li> </ul> |
| <b>Category</b>          | Displays the categorization of the address based on the location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Label</b>             | Displays a text description for classifying this contact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Alternative Label</b> | Displays a text description for classifying this contact. This is similar to <b>Label</b> , but it is used to store label in an alternate language.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Button     | Description                                     |
|------------|-------------------------------------------------|
| <b>Add</b> | Saves the modified information to the database. |

#### Related links

[Modifying the details of a public contact](#) on page 597

## Shared Address field descriptions

Use this page to create a new shared address and modify and delete an existing shared address.

### Shared Address

| Name                    | Description                                                                              |
|-------------------------|------------------------------------------------------------------------------------------|
| <b>Select check box</b> | Provides the option to select an address.                                                |
| <b>Name</b>             | Displays the name of the person or entity associated with the address.                   |
| <b>Address Type</b>     | Displays the type of address indicates whether the address is an Office or home address. |
| <b>Street</b>           | Displays the name of the street.                                                         |
| <b>City</b>             | Displays the name of the city or town.                                                   |

*Table continues...*

| Name               | Description                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Postal Code</b> | Displays the postal code used by postal services to route mail to a destination. In the United States, this is the Zip code. |
| <b>Province</b>    | Displays the full name of the province.                                                                                      |
| <b>Country</b>     | Displays the name of the country.                                                                                            |
| <b>Refresh</b>     | Refreshes the address information in the table.                                                                              |
| <b>All</b>         | Selects all the addresses in the table.                                                                                      |
| <b>None</b>        | Clears the check box selections.                                                                                             |

| Button        | Description                                                                              |
|---------------|------------------------------------------------------------------------------------------|
| <b>New</b>    | Displays the Add Address page. Use this page to add an address.                          |
| <b>Edit</b>   | Displays the Edit Address page. Use this page to modify the mailing address information. |
| <b>Delete</b> | Deletes a selected address.                                                              |

---

## Managing presence access control lists

---

### Manage Presence Access Control Lists

Default Policy rules are global default rules that define access to presence information if none of the more specific rules apply. You must define atleast one System Default rule in the system.

#### Related links

[Presence ACL field descriptions](#) on page 608

---

### Presence ACL field descriptions

#### Define Policy

You can use this section to define your personal rules for one or more watchers to access your presence information.

| Name                    | Description                                                      |
|-------------------------|------------------------------------------------------------------|
| <b>Select check box</b> | The option to select a rule.                                     |
| <b>Access Level</b>     | The presence information for which access control rules are set. |
| <b>Action</b>           | The access control permission for the presence information.      |

| Button        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| <b>Edit</b>   | Changes the existing rule.                                                    |
| <b>New</b>    | Adds a new rule for watchers.                                                 |
| <b>Delete</b> | Deletes the selected rule from the list of rules that are added for watchers. |

The page displays the following fields when you click **New** or **Edit**:

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access Level</b> | <p>The presence information for which access control rules are set.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Telephony</b>: The telephony-related presence information for which you can set an access permission.</li> <li>• <b>All</b>: All types of presence information for which you can set an access permission.</li> </ul>                                                                                                                                                                                                                                          |
| <b>Action</b>       | <p>The access control permission for the presence information.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>: Provides watcher the access to the presence information for the access level.</li> <li>• <b>Block</b>: Blocks the watcher from accessing the presence information for the access level.</li> <li>• <b>Confirm</b>: Watcher requires confirmation from the presentities to access the presence information of presentities.</li> <li>• <b>Undefined</b>: Access to the presence information for the access level is undefined for the watcher.</li> </ul> |

| Button      | Description                                                                             |
|-------------|-----------------------------------------------------------------------------------------|
| <b>Save</b> | Saves the rules information to the database when you add or change a rule for watchers. |

---

## Communication profile password policy enforcement

---

### Communication profile password policy

The system administrator defines a password strength policy for the communication profile password. The password has the following requirements:

- Passwords must contain 6 to 25 characters. The default value is 14.

- Passwords must contain a combination of the following characters: a-z, A-Z, 0-9, {, }, |, (, ), <, >, ,, /, ., =, [, ], ^, \_ ,@, !, \$, %, &, -, +, ", :, ?, `, or ;
- Passwords must contain at least one each of the following characters:
  - A lowercase letter
  - An uppercase letter
  - A number
  - A special character
- Password can contain maximum of 2 consecutive characters. The valid values are from 1 through 5. The default value is 2.
- Password can contain maximum number of 4 consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4.

If a password does not meet the password strength policy, the system rejects the password. You can disable the password policy.

#### Related links

[Editing the password policy for the communication profile](#) on page 610

[Communication Profile Password Policy field descriptions](#) on page 611

[User Profile | Add field descriptions](#) on page 295

---

## Editing the password policy for the communication profile

### Procedure

1. On the System Manager web console, click **Users > User Management > Communication Profile Password Policy**.
2. On the Communication Profile Password Policy page, do the following:
  - a. On the **Aging Policy** tab, select the **Enforce password aging policy** check box, and modify the required fields.
  - b. On the **History Policy** tab, select the **Enforce policy against previously used passwords** check box, and type the value in the **Previous passwords blocked** field.
  - c. On the **Strength Policy** tab, select the **Enforce password content standards** check box, and modify the required fields.

For information about the fields, see “Communication Profile Password Policy field descriptions”.

3. Click **Commit**.

System Manager saves the changes to the password policy for the communication profile password.

#### Related links

[Communication Profile Password Policy field descriptions](#) on page 611

## Communication Profile Password Policy field descriptions

### Aging Policy

| Name                                   | Description                                                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enforce password aging policy</b>   | <p>The option to enable or disable the password aging policies. By default, the password aging policy is disabled.</p> <p>To enforce the password aging policies, select the check box.</p> <p>If you clear the check box, the password aging policy is not applicable.</p> |
| <b>Expiration period</b>               | The maximum number of days to maintain the password. The default value is 60 days. The valid values are from 1 through 365 days.                                                                                                                                            |
| <b>Expiration warning</b>              | The number of days for password expiry prior to which the password expiration warning message must be sent to the user. The valid values are from 1 through 15 days. The default value is 10 days.                                                                          |
| <b>Minimum age for password change</b> | <p>The minimum number of days for password age. The valid values are from 0 through 7 days. The default value is 1 day.</p> <p>Ensure that the expiration period is greater than the minimum password age.</p>                                                              |
| <b>Enable expired password change</b>  | <p>If this is enabled, you can change the password after it expires.</p> <p>If this is disabled, only the system administrator can change the password. When you log in with the system administrator-provided password, you must change the password.</p>                  |

### History Policy

| Name                                                    | Description                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enforce policy against previously used passwords</b> | <p>The option to enable or disable the password policy against previously used passwords. By default, the password policy against previously used passwords is disabled.</p> <p>To enforce the password policy against previously used passwords, select the check box.</p> <p>If you clear the check box, the password policy against previously used passwords is not applicable.</p> |
| <b>Previous passwords blocked</b>                       | <p>The number of latest passwords that the system maintains in history. You cannot reset your password to these values. The valid values are from 1 through 15.</p> <p>From Release 8.1.3, the default value is 10.</p> <p>For earlier release system, the default value is 6.</p>                                                                                                      |

## Strength Policy

| Name                                                           | Description                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enforce password content standards</b>                      | <p>The option to enable or disable the password content standards. By default, the password content standards is disabled.</p> <p>To enforce the password content standards, select the check box.</p> <p>If you clear the check box, the password content standards is not applicable.</p>                                                                                            |
| <b>Minimum total length</b>                                    | <p>The minimum number of characters to use in the password. The password can be of 6 to 25 characters.</p> <p>From Release 8.1.3, the default value is 14.</p> <p>For earlier release system, the default value is 8.</p>                                                                                                                                                              |
| <b>Minimum by character Type: Lower case</b>                   | <p>The minimum number of lowercase characters to use in the password. The default value is 1.</p>                                                                                                                                                                                                                                                                                      |
| <b>Minimum by character Type: Upper case</b>                   | <p>The minimum number of uppercase characters to use in the password. The default value is 1.</p>                                                                                                                                                                                                                                                                                      |
| <b>Minimum by character Type: Numeric case</b>                 | <p>The minimum number of numeric characters to use in the password. The default value is 1.</p>                                                                                                                                                                                                                                                                                        |
| <b>Minimum by character Type: Special case</b>                 | <p>The minimum number of special characters to use in the password. The default value is 1.</p>                                                                                                                                                                                                                                                                                        |
| <b>Maximum repeated consecutive characters</b>                 | <p>The maximum number of repeated consecutive characters. The valid values are from 1 through 5. The default value is 2.</p> <p>For example, if the maximum repeated consecutive characters value is set to 2:</p> <ul style="list-style-type: none"> <li>Valid password is: Buildd123\$</li> <li>Invalid password is: Builddd123\$</li> </ul>                                         |
| <b>Maximum consecutive characters from same character type</b> | <p>The maximum number of consecutive characters from the same character type. The valid values are from 1 through 5. The default value is 4.</p> <p>For example, if the maximum repeated consecutive characters of the same character type is set to 4:</p> <ul style="list-style-type: none"> <li>Valid password is: Build123\$</li> <li>Invalid password is: Build12345\$</li> </ul> |

| Button        | Description                                                              |
|---------------|--------------------------------------------------------------------------|
| <b>Commit</b> | Saves all the changes on the Communication Profile Password Policy page. |
| <b>Cancel</b> | Cancels the changes and returns to the previous page.                    |

# Chapter 8: Managing user provisioning rules

---

## User Provisioning Rule

System Manager provides workflows to streamline the user provisioning process. You can apply a user provisioning rule with other LDAP Synchronization Capabilities to achieve fully automated user provisioning. You can also assign a communication profile to every user.

A user provisioning rule includes a master communication profile template and a set of provisioning rules. A user provisioning rule enables predefined templates that consist of user attributes found in the communication profile of the user. In the user provisioning rule, the administrator specifies the following information to provision the user:

- Basic information that includes the communication profile password, time zone, and language preference
- The communication system that the user must use, for example, Communication Manager
- The method to assign or create a communication profile for the user, for example, by assigning the next available extension for Communication Manager

When the administrator creates the user using the user provisioning rule, the system populates the following data based on the user provisioning rule:

- The default values
- The communication addresses
- The communication profiles for the user

You can create and apply the user provisioning rule only if you have administrator credentials. The administrator can assign only one user provisioning rule to every user. The administrator can provision the user using the user provisioning rule from one of the following System Manager user interfaces:

- Web Console
- Web Services
- Folder name Synchronization
- Bulk import

**\* Note:**

To perform the user provisioning by using the user provisioning rule, map the user to the role with the following permissions:

| Resource type                 | Permissions |
|-------------------------------|-------------|
| All elements of type:elements | view        |

---

## Capabilities and guidelines of user provisioning rules

### Capabilities of user provisioning rules

The user provisioning rule is a template that is used to create a user. You can define and apply a user provisioning rule only if you have administrator credentials. You can use the user provisioning rule for the initial provisioning and while creating the user. User provisioning rules cannot be used after they are applied. After you create a user by using a user provisioning rule, System Manager populates the following data based on the rules defined in the user provisioning rule:

- The default values
- The communication addresses
- The user attributes from the communication profiles

### General guidelines

- After you define a user provisioning rule and apply the rule to create a user, you cannot edit the communication profile associated with the user provisioning rule. You cannot change, delete, or add the data in the communication profile by using the user provisioning rule. You can assign only one communication profile to a user provisioning rule.

**\* Note:**

When you define user provisioning rule with elements data in the **Communication Profile** section, and later if you change value for Session Manager, Communication Manager Templates, and Messaging elements, then you must update the existing user provisioning rule with latest element data.

If the user provisioning rule and communication profile data are available from the System Manager user interface or bulk import, the communication profile data that you provide takes the precedence. System Manager does not use the communication profile data from the user provisioning rule.

- After you create the user by using the user provisioning rule, you can modify values of an existing communication profile by using one of the following System Manager user provisioning interfaces:
  - System Manager native user interface
  - Web Services API
  - Bulk import and export
  - Global Endpoint Change Editor

Also, you can add another communication profile by using a different user provisioning rule.



- Whenever a user provisioning rule is used while creating or updating a user, the administrator should not manually remove any communication profile.

### **Guidelines for upgrading Communication Manager and Messaging elements**

1. Before upgrading the Communication Manager and Messaging elements to major Release 6.3.x and later, note down the Communication Manager and Messaging templates associated with user provisioning rule in System Manager.
2. Once the Communication Manager or Messaging element is upgraded, then templates associated with old release of Communication Manager and Messaging will get unlinked for existing user provisioning rule. Therefore, after upgrading Communication Manager and Messaging elements:
  - a. Create custom templates for the current release of Communication Manager and Messaging.
  - b. Update existing user provisioning rule with newly created custom templates or default templates of Communication Manager and Messaging as per the user provisioning rule guidelines.

---

## **Adding User Provisioning Rules**

### **About this task**

Add a service defined in a communications profile to an existing user that was created by using a user provisioning rule.

### **Procedure**

1. Create a new user provisioning rule with the new service defined in the communication profile of the new rule.

The system adds the new service defined in the communications profile to the existing user.

You can add any of the following services:

- Presence
  - Messaging
  - Avaya Breeze® platform
2. Apply the user provisioning rule to the user through LDAP synchronization.
  3. Update the LDAP enterprise directory with the new user provisioning rule.
  4. Synchronize users.

The system creates a new communication profile for the user.

---

## Creating the user provisioning rule

### Procedure

1. Log on to System Manager with administrator privilege credentials.
  2. On the System Manager web console, click **Users > User Provisioning Rule**.
  3. On the User Provisioning Rules page, click **New**.
  4. On the New User Provisioning Rule page, do the following:
    - a. On the **Basic** tab, enter the appropriate information.
    - b. On the **Communication Profile** tab, select the appropriate communication profile, and enter the appropriate information.
    - c. On the **Organization** tab, enter the appropriate information.
- For more information, see “User Provisioning Rule field descriptions”.
5. Click **Commit** to save the changes.

### Related links

[New User Provisioning Rule field descriptions](#) on page 619

---

## Modifying the user provisioning rule

### Before you begin

Create a user provisioning rule.

### Procedure

1. Log on to System Manager with administrator privilege credentials.
2. On the System Manager web console, click **Users > User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule.
4. To edit the user provisioning rule, click one of the following:
  - **Edit**.
  - **View > Edit**.
5. On the Edit User Provisioning Rule page, do the following:
  - a. On the **Basic** tab, modify the appropriate information.



#### Note:

- System Manager does not automatically modify the user if the user provisioning rule changes.

- You can select a different user provisioning rule when you modify the user information.
- b. On the **Communication Profile** tab, modify the communication profile information as appropriate.
- c. On the **Organization** tab, modify the appropriate information.

For information, see “User Provisioning Rule field descriptions”.

6. Click **Commit**.

#### Related links

[New User Provisioning Rule field descriptions](#) on page 619

---

## Viewing the user provisioning rule

### Before you begin

Create a user provisioning rule.

### Procedure

1. Log on to System Manager with administrator privilege credentials.
2. On the System Manager web console, click **Users > User Provisioning Rule**.
3. On the User Provisioning Rules page, select the user provisioning rule, and click **View**.

#### Related links

[New User Provisioning Rule field descriptions](#) on page 619

---

## Creating a duplicate user provisioning rule

### About this task

You can create a new user provisioning rule by duplicating the information from an existing user provisioning rule.

### Procedure

1. Log on to System Manager with administrator privilege credentials.
2. On the System Manager web console, click **Users > User Provisioning Rule**.
3. On the User Provisioning Rules page, click the user provisioning rule.
4. Click **Duplicate**.

5. On the Duplicate User Provisioning Rule page, do the following:
  - a. On the **Basic** tab, change the appropriate information.
  - b. On the **Communication Profile** tab, change the communication profile information as appropriate.
  - c. On the **Organization** tab, change the appropriate information.For more information, see “User Provisioning Rule field descriptions”.
6. Click **Commit**.

#### Related links

[New User Provisioning Rule field descriptions](#) on page 619

---

## Deleting a user provisioning rule

### Procedure

1. Log on to System Manager with administrator privilege credentials.
2. On the System Manager web console, click **Users > User Provisioning Rule**.
3. On the User Provisioning Rules page, select one or more user provisioning rules.
4. Click **Delete**.
5. On the Delete User Provisioning Rule page, click **Delete**.

System Manager:

- Removes the selected user provisioning rule.
- Disassociates the user provisioning rule from the user if you have already provided the user provisioning rule for the user.

#### Related links

[New User Provisioning Rule field descriptions](#) on page 619

---

## User Provisioning Rules field descriptions

| Name               | Description                                    |
|--------------------|------------------------------------------------|
| <b>Name</b>        | The name of the user provisioning rule.        |
| <b>SIP Domain</b>  | The name of the configured SIP domain name.    |
| <b>Description</b> | The description of the user provisioning rule. |

| Button           | Description                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View</b>      | Displays the View User Provisioning Rule page with details of the user provisioning rule that you selected.                                                                                                                                 |
| <b>Edit</b>      | Displays the Edit User Provisioning Rule page where you can modify the selected rule.                                                                                                                                                       |
| <b>New</b>       | Displays the New User Provisioning Rule page where you can create a new rule.                                                                                                                                                               |
| <b>Delete</b>    | Deletes the selected user provisioning rule.                                                                                                                                                                                                |
| <b>Duplicate</b> | Duplicates the selected user provisioning rule.                                                                                                                                                                                             |
| <b>Select</b>    | <p>Selects a user provisioning rule in the table. The options are:</p> <ul style="list-style-type: none"> <li>• <b>All</b>: To select all user provisioning rules in the table.</li> <li>• <b>None</b>: To clear the selections.</li> </ul> |

| Icon                                                                              | Name    | Description                                                    |
|-----------------------------------------------------------------------------------|---------|----------------------------------------------------------------|
|  | Refresh | Refreshes the user provisioning rule information in the table. |

## New User Provisioning Rule field descriptions

### Basic

| Name                               | Description                                                                                                                                                                                                                                                                                            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Provisioning Rule Name</b> | The name of the user provisioning rule.                                                                                                                                                                                                                                                                |
| <b>Description</b>                 | A description of the user provisioning rule.                                                                                                                                                                                                                                                           |
| <b>SIP Domain</b>                  | <p>The name of the configured SIP domain name.</p> <p>If <b>SIP Domain</b> is nonblank, create an Avaya SIP communication address for the user.</p> <p>The system changes the SIP domain for all selected users with the value that you provide in this field.</p>                                     |
| <b>Presence/IM Domain</b>          | <p>The name of the configured Presence domain name.</p> <p>If <b>Presence/IM Domain</b> is nonblank, create an Avaya Presence/IM communication address for the user.</p> <p>The system changes the Presence/IM Domain domain for all selected users with the value that you provide in this field.</p> |

*Table continues...*

| Name                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Communication Profile Password</b>                   | <p>The communication profile password.</p> <p>The field is available only if you enable the communication profile. The password policy is configured on the <b>Users &gt; User Management &gt; Communication Profile Password Policy</b> page.</p> <p>When you provide the communication password value during bulk edit of users, the system overwrites any existing communication profile passwords of the user.</p>                                                                                          |
| <b>Confirm Password</b>                                 | The communication profile password that you must re-enter.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Use Phone Number last ..... digits for Extension</b> | <p>The number of last digits of the phone number that the system uses from the LDAP attribute.</p> <p>E.164 numbers can contain maximum 13 digits. Usually, the numbers are written with a plus (+) as the prefix. The system populates the phone number that is mapped to the LDAP attribute with the value in the <b>Prefix for Avaya E164 Handle</b> field.</p> <p>The LDAP attribute is mapped to the <code>PhoneNumber</code> attribute of System Manager on the User Synchronization Datasource page.</p> |
| <b>Prefix for Avaya E164 Handle</b>                     | The digits that the system must prefix to the telephone number or Avaya E.164 handle. The default is plus (+).                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Language Preference</b>                              | The preferred written or spoken language of the user. For example, English.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Time Zone</b>                                        | The preferred time zone of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Button        | Description                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Creates the user provisioning rule and displays the User Provisioning Rule page.                                                             |
| <b>Cancel</b> | Cancels the create, edit, or delete operation of the user provisioning rule.                                                                 |
| <b>Done</b>   | <p>Saves the changes that you make to the user provisioning rule.</p> <p>The system displays this button only during the view operation.</p> |
| <b>Edit</b>   | <p>Displays the fields in the edit mode.</p> <p>The system displays this button only during the view operation.</p>                          |

**Communication Profile tab: Session Manager Profile****\* Note:**

The system displays the following fields only if a communication profile of the user exists for the product:

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Session Manager</b>   | The instance that you want to use as the home server for the currently displayed communication profile. As a home server, the selected primary Session Manager instance is used as the default access point for connecting devices associated with the communication profile to the Avaya Aura <sup>®</sup> network. You must select the primary Session Manager server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Secondary Session Manager</b> | The Session Manager instance that you select as the secondary Session Manager. It provides continued service to SIP devices associated with this communication profile when the primary Session Manager server becomes unavailable. A selection is optional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Survivability Server</b>      | <p>For local survivability, you can specify a survivability server to provide survivability communication services for devices associated with a communication profile when the local connectivity to Session Manager instances in Avaya is lost. If you select Branch Session Manager, and the termination and origination application sequences contain a Communication Manager application, sequencing to this application continues, locally, to Communication Manager survivable remote server resident with Branch Session Manager. A selection is optional.</p> <p><b>* Note:</b></p> <p>If a termination or origination application sequence contains a Communication Manager application, the Communication Manager instance associated with the application must be the main server for the Communication Manager survivable remote server that resides with Branch Session Manager.</p> <p>After typing minimum of 3 characters, wait for three seconds to capture the final keyword, and fetch the required results.</p> |

*Table continues...*

| Name                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max. Simultaneous Devices</b>                                | The maximum number of endpoints that you can register at a time by using this communication profile. If you register more than one endpoint, all the endpoints receive calls simultaneously.                                                                                                                                                                                                                                          |
| <b>Block New Registration When Maximum Registrations Active</b> | If you select the check box and an endpoint attempts to register using this communication profile after the registration requests exceed the administered limit, the system denies any new registrations with Session Manager. The system sends a warning message and stops the SIP service to the endpoint.                                                                                                                          |
| <b>Origination Application Sequence</b>                         | <p>The application sequence that the system invokes when routing calls from this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p>   |
| <b>Termination Application Sequence</b>                         | <p>The application sequence that is invoked when the system routes calls to this user. A selection is optional.</p> <p> <b>Note:</b></p> <p>If you specify origination and termination application sequences, and if each sequence contains a Communication Manager application, Communication Manager must be the same in both the sequences.</p> |
| <b>Emergency Calling Origination Sequence</b>                   | The list of application sequences invoked when the system routes emergency calls from this user.                                                                                                                                                                                                                                                                                                                                      |
| <b>Emergency Calling Termination Sequence</b>                   | The list of application sequences invoked when the system routes emergency calls to this user.                                                                                                                                                                                                                                                                                                                                        |
| <b>Home Location</b>                                            | The home location to support mobility for the currently displayed user. Session Manager uses the home location specifically when the IP address of the calling phone does not match the IP Address Pattern of any location. You must specify a value.                                                                                                                                                                                 |
| <b>Conference Factory Set</b>                                   | <p>The conference factory set to enable media capability-based call routing to the Conferencing SIP entities.</p> <p>Use the <b>Session Manager &gt; Application Configuration &gt; Conference Factories</b> webpage to administer the Conference Factory Sets.</p>                                                                                                                                                                   |



**Communication Profile tab: Avaya Breeze® platform Profile**

| Name                   | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Service Profile</b> | The profile that you assign to the user. The user can gain access to the service contained in the profile. |

**Communication Profile tab: CM Endpoint Profile****\* Note:**

The system displays these fields only if a Communication Manager Endpoint profile exists for the user.

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use Next Available Extension</b> | <p>The option to instruct the system to create a new extension for the user.</p> <p><b>* Note:</b><br/>For LDAP synchronization, the value in the <b>Use Phone Number last ..... digits for Extension</b> field takes priority.</p>                                                                                                                                                           |
| <b>Template</b>                     | The template, system defined or user defined, that you associate with the endpoint. Select the template based on the set type you add.                                                                                                                                                                                                                                                        |
| <b>Sub Type</b>                     | This field is configured for CS 1000 station types only. You can select the specific set for <b>Set Type</b> . On the Manage Endpoint page, <b>Sub Type</b> is labeled as <b>Set</b> .                                                                                                                                                                                                        |
| <b>System ID</b>                    | <p>This field is configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0 more than one station can use the combination of <b>System ID</b> and <b>Terminal Number</b>.</p> <p>With Release 8.0.1, each station must have a unique combination of <b>System ID</b> and <b>Terminal Number</b>.</p> |
| <b>Security Code</b>                | The security code for authorized access to the endpoint.                                                                                                                                                                                                                                                                                                                                      |
| <b>Preferred Handle</b>             | Avaya SIP or Avaya E.164 handle that is administered for the user. The field is optional. By default, the field is blank.                                                                                                                                                                                                                                                                     |
| <b>Password</b>                     | <p>The password to gain access to the endpoint.</p> <p>The system displays the field if you select <b>Agent</b> in <b>Profile Type</b>.</p>                                                                                                                                                                                                                                                   |

*Table continues...*

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Allow H.323 and SIP Endpoint Dual Registration</b> | The option to register an H.323 endpoint and a SIP endpoint together at the same time to the same extension. For more information about the SIP and H.323 dual registration feature, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> on the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a> . |

### Communication Profile tab: CS 1000 Endpoint Profile

| Name                                                     | Description                                                                                                                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                            | The system that will be the element manager of the CS 1000 endpoint profile. You must select the system.                                  |
| <b>Target</b>                                            | The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. |
| <b>Template</b>                                          | The phone or endpoint template that you can choose for the user. The element manager maintains all templates. You must select a template. |
| <b>Include in Corporate Directory</b>                    | The option to add this profile to the CS 1000 Corporate Directory feature.                                                                |
| <b>Delete Endpoint on Unassign of Endpoint from User</b> | An option to specify whether to delete the endpoint from the CS 1000 system when you unassign the endpoint from the user.                 |

### Communication Profile tab: Messaging Profile

 **Note:**

The system displays the following fields only if you can configure a messaging profile for the user

| Name                  | Description                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>         | The messaging system on which you add the subscriber. You must select the system.                                                                                                                                                                                                                                                                                          |
| <b>Mailbox Number</b> | The mailbox number of the subscriber. The options are: <ul style="list-style-type: none"> <li>• Use CM Extension: Use this option only if the Communication Manager profile and Session Manager profile are specified.</li> <li>• Use Next Available Subscriber: Use this option if the system must use the next mailbox number to associate with this profile.</li> </ul> |

*Table continues...*

| Name                                                                           | Description                                                                                                                                                                            |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Template</b>                                                                | The system-defined or user-defined template that you associate with the subscriber.                                                                                                    |
| <b>Password</b>                                                                | The password for logging in to the mailbox. You must provide the password.                                                                                                             |
| <b>Delete Subscriber on Unassign of Subscriber from User or on Delete User</b> | The option to specify whether to delete the subscriber mailbox from the Messaging device or Communication System Management when you remove this Messaging profile or delete the user. |

### Communication Profile tab: Avaya Messaging Profile

| Name                              | Description                                                                                                                                                                                                                                                                               |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                     | The Avaya Messaging system to which you add a mailbox.                                                                                                                                                                                                                                    |
| <b>Refresh</b>                    | <p>The option to get information about company, departments, and feature groups from Avaya Messaging and save locally on System Manager for future use.</p> <p>You do not require to refresh for every user.</p>                                                                          |
| <b>Use Next Available Mailbox</b> | The option to specify if the system must use the next mailbox number to associate with this profile.                                                                                                                                                                                      |
| <b>Mailbox Range</b>              | <p>The range of mailbox numbers assigned to the Avaya Messaging system.</p> <p> <b>Note:</b></p> <p>This option is available only when you select the <b>Use Next Available Mailbox</b> check box.</p> |
| <b>Numeric Password</b>           | The numeric password that is used to log in to the Avaya Messaging system.                                                                                                                                                                                                                |
| <b>Application User Password</b>  | The password that is used to gain access to non-telephone applications, such as Web Client, iLink Pro, iLink Pro Mobile, and iLink Pro Desktop.                                                                                                                                           |
| <b>Company</b>                    | The name of the company to which the user belongs.                                                                                                                                                                                                                                        |
| <b>Department</b>                 | The department to which the user belongs.                                                                                                                                                                                                                                                 |
| <b>Feature Group</b>              | The feature group name that determines the rules for the mailboxes associated with it.                                                                                                                                                                                                    |

*Table continues...*

| Name                             | Description                                                                                                                                                                                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Capability</b>                | <p>The type of functionality that the user contains. The values are:</p> <ul style="list-style-type: none"> <li>• <b>Standard</b></li> <li>• <b>Fax</b></li> <li>• <b>Messaging</b></li> <li>• <b>Collaboration</b></li> <li>• <b>Messaging and Collaboration</b></li> </ul> |
| <b>Domain Account Name</b>       | <p>The mailbox NT account name for the Avaya Messaging profile. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Same as Login Name</b></li> <li>• <b>Admin Specified</b></li> </ul>                                                                         |
| <b>Synchronization User Name</b> | <p>The account name that is used to gain access to the email server, for example, Microsoft Exchange and Google Gmail.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Same as Login Name</b></li> <li>• <b>Admin Specified</b></li> </ul>           |

### Communication Profile tab: IP Office Endpoint Profile

| Name             | Description                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>    | The list of IP Office device names from which you can select the IP Office device that you associate with the user. You must select the template.                                                                                                                                                                                                                                    |
| <b>Extension</b> | <p>The extension of the endpoint to which you associate the profile. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Use CM Extension:</b> Use this option only if Communication Manager profile is specified.</li> <li>• <b>Use Next Available Extension:</b> Use this option if the system must use the next extension to associate with this profile.</li> </ul> |
| <b>Template</b>  | A list of user templates from which you can select a template to set the user configurations.                                                                                                                                                                                                                                                                                        |
| <b>Set Type</b>  | The set type for the IP Office endpoint profile. By default, the <b>Set Type</b> field is disabled. If you select a template, the system automatically populates the set type value.                                                                                                                                                                                                 |

**Communication Profile tab: Presence Profile**

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                              | The Presence Services instance that is the home Presence Services server for the user. You must select an instance. As a home server, the Presence Services instance can perform the following for the communication profile: <ul style="list-style-type: none"> <li>• Aggregate presence</li> <li>• Archive instant messages if the Instant Messages option is enabled</li> </ul>      |
| <b>SIP Entity</b>                          | The option to route the SIP-based messages through Presence Services. This system selects the SIP entity only if you select a Presence Services instance in the <b>System</b> field. <b>SIP Entity</b> is read-only. If the system cannot identify a SIP entity, an appropriate error message is displayed in the field.                                                                |
| <b>IM Gateway SIP Entity</b>               | The Presence Services instance for the user.                                                                                                                                                                                                                                                                                                                                            |
| <b>Publish Presence with AES Collector</b> | The option that determines if Presence Services must publish presence with AES Collector. The options are: <ul style="list-style-type: none"> <li>• <b>System Default</b></li> <li>• <b>Off</b></li> <li>• <b>On</b></li> </ul> The default is <b>System Default</b> . You can change the default value. You do not require to configure AES Collector in the Presence Services server. |

**Communication Profile tab: Conferencing Profile**

| Name/Button                                                   | Description                                                                                                                                                                                    |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Template</b>                                               | The template that you use to set the user configurations.                                                                                                                                      |
| <b>Location</b>                                               | The location that Conferencing uses when the IP address of the calling phone does not match any IP address pattern of any location.<br>Specify this field to support the mobility of the user. |
| <b>Select Auto-generated Code Length</b>                      | The number of digits in the security code that the system generates.                                                                                                                           |
| <b>Auto Generate Participant and Moderator Security Codes</b> | The check box that you select to instruct the system to generate the security codes for the participant and moderator.                                                                         |

**Communication Profile tab: Equinox Profile**

| Name/Button                  | Description                                                                   |
|------------------------------|-------------------------------------------------------------------------------|
| <b>Equinox User Password</b> | The password that is used to log in to the Avaya Workplace Client Management. |

*Table continues...*

| Name/Button                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Virtual Room Number</b> | <p>The number of a virtual room that is used to create a conference.</p> <p>By default Virtual Room Number serves as Meeting ID when a conference is created. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Use Phone Number:</b> This will use Communication Manager extension. Use this option only if Communication Manager profile is already associated with the user or being associated with the user.</li> <li>• <b>Auto Generate Virtual Room Number:</b> Use this option if the system needs to generate the Virtual Room Number automatically.</li> </ul> |

## Organization

| Name/Button       | Description                                                       |
|-------------------|-------------------------------------------------------------------|
| <b>Tenant</b>     | The tenant of the user created by the user provisioning rule.     |
| <b>Site</b>       | The work site of the user created by the user provisioning rule.  |
| <b>Department</b> | The department of the user created by the user provisioning rule. |
| <b>Team</b>       | The team of the user created by the user provisioning rule.       |

| Button        | Description                                                          |
|---------------|----------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes and displays the User Provisioning Rules page.     |
| <b>Cancel</b> | Cancels the operation and displays the User Provisioning Rules page. |

# Chapter 9: Managing elements

---

## Importing users from Subscriber Manager to User Management

---

### User data import to System Manager

The User Profile Management (UPM) service in System Manager is a single point of administration for user profile data associated with multiple Avaya products. Similarly, the Subscriber Manager service in CS 1000 UCM is a single point of administration for user profile data for Heritage Nortel products. In System Manager 6.1, the UPM and Subscriber Manager applications coexist and are part of System Manager. Element Managers use:

- UPM to manage users for Heritage Avaya products
- Subscriber Manager to manage users for Heritage Nortel products

In System Manager 6.2, Subscriber Manager is merged into UPM and is called User Management (UM). UM includes several Subscriber Manager features. With the removal of Subscriber Manager, perform the steps listed in this section on System Manager 6.1 and 6.2 or later to ensure that the subscriber data is successfully migrated to UM of System Manager 6.2 and later.

#### Prerequisites

Register CS 1000 with the preupgraded System Manager Release 6.1 primary security domain.

Moving users and accounts from Subscriber Manager to User Management involves the following key procedures:

- On System Manager Release 6.1: Preparing the Subscriber Manager user data for import to User Management. This preimport procedure copies the Subscriber Manager Universally Unique ID (UUID) of the user to another field which can be preserved during the import to User Management. After the import, you must use the UUID to reassociate phones and mailboxes.
- On System Manager Release 6.1: Importing the Subscriber Manager user data to User Management. This procedure transfers the user data from the Subscriber Manager directory to the User Management database using LDAP synchronization.
- On System Manager Release 6.2 and later: Performing postimport tasks that involve:
  - Exporting the users to an XML file to assign communication profile passwords in User Management and reimporting the users.

- Creating the communication profile for each user and performing profile synchronization in User Management for CS 1000 element that you import.

---

## Preparing the Subscriber Manager user data for import to User Management

You must perform this procedure on System Manager Release 6.1.

### Before you begin

- Ensure that you install the latest CS 1000 Service Pack on all the CS 1000 network elements.
- Ensure that you update all Subscriber Manager user profiles for completeness that includes First Name, Last Name, and Preferred Name / CPND Name.
- Ensure that you synchronize Subscriber Manager and the CS 1000 network elements and that you upload Corporate Directory and Numbering Groups to the CS 1000 network elements.
- Ensure that the firewall is stopped on System Manager Release 6.1. Perform the following to verify that the firewall is stopped:
  1. Using the command line interface, log in to System Manager Release 6.1 as `root`.
  2. Enter `service iptables status`.  
The system must indicate that the firewall service has stopped.
  3. If firewall is enabled, enter `service iptables stop`.  
The system stops the firewall service.

### Procedure

1. Log on to the Web console of System Manager Release 6.1.
2. On the Avaya Unified Communications Management page, click **Network > Subscriber Manager**.
3. In the left navigation pane, click **CSV Export**.
4. Click **Generate** on the upper-right of the page to create a new CSV file with the latest subscriber data.
5. Click **Download** on the upper-right of the page to download the subscriber data to your computer.  
Note the location of the `subscribers.csv` file.
6. Open the `subscribers.csv` file using Microsoft Excel and perform the following steps:
  - a. Copy the data from the **UUID** column to the **postOfficeBox** column, without the column header information. This is to ensure that the Subscriber Manager datastore UUID is mapped to a column that the UPM LDAP datastore synchronization supports. For example:



| entryUUID                            | postOfficeBox                        |
|--------------------------------------|--------------------------------------|
| c0bbc2d2-3096-4ce8-8fca-2670ea681be3 | c0bbc2d2-3096-4ce8-8fca-2670ea681be3 |
| 86d11715-3b36-4238-be37-5284ca7a7a68 | 86d11715-3b36-4238-be37-5284ca7a7a68 |

- b. Copy the data from the **ucDomain** to the **User ID (uid)** column. For example:

| ucDomain     | uid                |
|--------------|--------------------|
| ca.avaya.com | user1@ca.avaya.com |
| ca.avaya.com | user2@ca.avaya.com |

- c. Save the modified `subscribers.csv` file in a csv format.
7. To synchronize the Subscriber Manager data with the modified `subscribers.csv` file, import the modified Subscriber Manager data in the `subscribers.csv` file back to Subscriber Manager and perform the following steps:
- In the left navigation panel, on the **Subscriber Manager**, click **CSV Synchronization**.
  - Browse to the location where you saved the modified `subscribers.csv` file.
  - Click **Synchronize**.
  - Click **View Results** to verify that the synchronization is successful.
- If error occurs, the page displays the location of the error logs on the System Manager server. For example, `/opt/nortel/cnd/log/LDAP_Sync`.
- Click **Subscribers**, leave the **Name** field blank, and click **Search**.
  - Select one of the user and verify that the system updated the **Unified Communication Username** field correctly.
- The system does not display the **postOfficeBox** field.
8. If Numbering Groups are used, perform the following:
- Click **UCM Services > Numbering Groups**.
  - Click **Generate**.
  - Click **Export** to export the data to a location on your computer to ensure that the data is captured.

## Importing the Subscriber Manager user data to User Management

### Before you begin

- Log on to the web console of System Manager Release 6.1.
- Prepare the Subscriber Manager user data for import to User Management.

### Procedure

- On the System Manager web console, click **Users > Synchronize and Import**.

2. In the navigation pane, click **Sync Users**.
3. To create a new LDAP synchronization source, on the **Synchronization Datasources** tab, click **New** and enter the directory parameters as listed in the Subscriber Manager datasource parameters and attributes table.

Directory Parameters

|                           |                           |
|---------------------------|---------------------------|
| * Datasource Name         | cn                        |
| * Host                    | localhost                 |
| * Principal               | uid=admin,ou=People,dc=   |
| * Password                |                           |
| * Port                    | 389                       |
| * Base Distinguished Name | dc=nortel,dc=com          |
| * LDAP User Schema        | inetOrgPerson             |
| * Search Filter           | (objectClass=nortelSubscr |
| Use SSL                   | <input type="checkbox"/>  |
| Allow Deletions           | <input type="checkbox"/>  |
| Allow Null values in LDAP | <input type="checkbox"/>  |
| Test Connection           |                           |

---

Attribute Parameters

|               |                  |
|---------------|------------------|
| Add Mapping   |                  |
| postOfficeBox | -> sourceUserKey |
| uid           | -> loginName     |
| sn            | -> surname       |
| givenName     | -> givenName     |
| displayName   | -> displayName   |

**\* Note:**

If a subscriber does not have an account or the **cpndName** field is blank, you can map Last name, First Name to the displayName attribute of System Manager.

4. Click **Test Connection** to verify that the system can establish connection to the cn database.
5. Perform the following steps to run the LDAP synchronization job:
  - a. On the Sync Users page, on the **Active Synchronization Jobs** tab, click **Create New Job**.
  - b. On the New User Synchronization Job page, in the **Datasource Name** field , select the name of the datasource and click **Run Job**.

The system starts the synchronization of the Subscriber Manager datastore with the User Management datastore.

6. On the Sync Users page, on the **Synchronization Job History** tab, click **View Job Summary** for the cn job, and verify that the system successfully imported the users in the **Added** and **Modified** fields.

**\* Note:**

The **Failed** field might contain some errors due to the import of unsupported fields.

7. To verify that the users are available in User Management, do the following:

- a. Navigate to **Users > User Management > Manage Users**.
- b. On the User Management page, select a user and click **View** or **Edit** and verify that the System Manager Release 6.1 is configured correctly.

System Manager Release 6.1 now contains User Management configured with the Subscriber Manager data. The system is now ready for upgrading to System Manager Release 6.2 and later.

### Related links

[Creating the user synchronization job](#) on page 91

[Adding the synchronization datasource](#) on page 82

[Subscriber Manager datasource parameters and attributes](#) on page 633

## Subscriber Manager datasource parameters and attributes

Use the values from the following tables to update the fields on the Edit User Synchronization Datasource page.

### Directory Parameters

| Parameter                        | Value                                                           |
|----------------------------------|-----------------------------------------------------------------|
| <b>Datasource Name</b>           | cnd                                                             |
| <b>Host</b>                      | For UPM: localhost<br>For CS 1000: <CS 1000 UCM R7.X Server IP> |
| <b>Principal</b>                 | applicationName=subMgr,ou=Applications,dc=Nortel,dc=com         |
| <b>Password</b>                  | submgrpass                                                      |
| <b>Port</b>                      | 389                                                             |
| <b>Base Distinguished Name</b>   | dc=nortel,dc=com                                                |
| <b>LDAP User Schema</b>          | inetOrgPerson                                                   |
| <b>Search Filter</b>             | (objectClass=nortelSubscriber)                                  |
| <b>Use SSL</b>                   | Clear the check box                                             |
| <b>Allow Deletions</b>           | Clear the check box                                             |
| <b>Allow Null values in LDAP</b> | Clear the check box                                             |

### Attribute Parameters

Map the following attributes of the Subscriber Manager datasource to the attributes of the User Management datastore.

| Subscriber Manager attribute | User Management attribute | Import Type | Description                                    |
|------------------------------|---------------------------|-------------|------------------------------------------------|
| uid                          | loginName                 | text        | Modified Subscriber Manager uid: user1@domain. |
| sn                           | surname                   | text        |                                                |
| postOfficeBox                | sourceUserKey             | text        | Saved Subscriber Manager UUID.                 |
| givenName                    | givenName                 | text        |                                                |
| displayName                  | displayName               | text        |                                                |

## Exporting the user data and creating the user profile

To complete the import job of the user data from Subscriber Manager, you must perform the following procedure after you complete the server upgrade from System Manager Release 6.1 to Release 6.2 and later.

### Before you begin

Start an SSH session.

### About this task

The system does not support the export of users and user profiles in bulk from the web console of System Manager Release 6.2 and release earlier than 6.3.8. Therefore, use the command line interface of System Manager to perform bulk export activities.

### Procedure

1. Log on to the system on which you want to export the user data as root.
2. Export the users and the user profiles using the following steps:
  - a. Perform one of the following:
    - For System Manager 6.3.8 and later, use the web console to export the user data.  
For more information, see [Exporting users in bulk](#).
    - For System Manager 6.3, type `cd $MGMT_HOME/bulkadministration/exportutility/`.
    - For System Manager 6.2, type `$MGMT_HOME/upm/bulkexport/exportutility/`.
  - b. For System Manager release earlier than 6.3.8, type `sh exportUpmUsers.sh`.  
The system creates an XML file `exportfile_<time stamp in milliseconds>.zip` in the `$MGMT_HOME/upm/bulkexport/` location.
3. Copy the zip file on the desktop of your local computer and extract the XML file.  
Note the location where you saved the file.

## 4. Make the following edits to the XML file:

- a. Add the `<commPassword>password_value</commPassword>` tag after the `<userName>` tag to assign the communication profile password in User Management.

 **Note:**

The password must have at least seven characters and the first character must not be a digit or a special character such as `<`, `>`, `^`, `%`, `$`, `@`, `#` and `*`.

- b. Delete the `<userPassword>userpassword_value</userPassword>` tag.

For example:

```
<tns:user>
 <authenticationType>enterprise</authenticationType>
 <displayName>user1</displayName>
 <displayNameAscii>user1</displayNameAscii>
 <dn>cn=f225860c-2f2c-4290-
a660-660e51fe0d4f,ou=Subscribers,dc=nortel,dc=com</dn>
 <isDuplicatedLoginAllowed>false</isDuplicatedLoginAllowed>
 <isEnabled>true</isEnabled>
 <isVirtualUser>false</isVirtualUser>
 <givenName>first1</givenName>
 <loginName>user1@ca.avaya.com</loginName>
 <preferredLanguage>en-US</preferredLanguage>
 <source>cnd</source>
 <sourceUserKey>c0bbc2d2-3096-4ce8-8fca-2670ea681be3</sourceUserKey>
 <status>provisioned</status>
 <surname>last1</surname>
 <userName>user1</userName>

 <commPassword>123456</commPassword>

 <roles>
 <role>End-User</role>
 </roles>
 <ownedContactLists>
 <contactList>
 <name>list-user1_ca.avaya.com</name>
 <isPublic>false</isPublic>
 <contactListType>general</contactListType>
 </contactList>
 </ownedContactLists>
 <commProfileSet>
 <commProfileSetName>Primary</commProfileSetName>
 <isPrimary>true</isPrimary>
 </commProfileSet>
</tns:user>
```

## 5. Reimport the user data from the modified XML files to the Import users page on the web console.

You can navigate to the Import users page from **Services > Bulk Import and Export > Import > User Management > Users** on the web console. For more information, see Bulk importing of users.

 **Note:**

The system might display an error message when you reimport the modified user data for admin user because the XML file includes the admin user when you export the user data. Ignore the message because you cannot edit the data for the admin user.

6. To create a user profile, synchronize profile in User Management for CS 1000 element that are being imported. For information on profile synchronization, see Synchronizing CS 1000 profiles.

**Related links**

[Bulk importing of users](#) on page 379

[Exporting users in bulk from web console](#) on page 383

---

## Importing users from CS 1000 Subscriber Manager to User Management

---

### CS 1000 Subscriber Manager data import options

If CS 1000 Release 7.x is available while installing System Manager 6.2 or later, you can import the CS 1000 Release 7.x Subscriber Manager user data into System Manager User Management.

Use one of the following options to import the CS 1000 Subscriber Manager data:

- Using the active primary CS 1000 Subscriber Manager server to LDAP synchronize the Subscriber Manager data.
- Using the CND or LDAP Data Interchange Format (LDIF) output to capture the CS 1000 Subscriber Manager data.

---

### Preparing the CS 1000 Subscriber Manager user data for import to System Manager

This option uses the active primary CS 1000 Subscriber Manager server for System Manager User Management to perform an LDAP synchronization of the user data.

**Procedure**

1. Log in to the primary CS 1000 UCM server command line using one of the following user names:
  - For CS 1000 Release 7.5 systems, admin2
  - For CS 1000 Release 7.0 and later systems, nortel

2. On the CS 1000 Release 7.x UCM server, perform the steps outlined in Preparing the Subscriber Manager user data for import to User Management.

#### Related links

[Preparing the Subscriber Manager user data for import to User Management](#) on page 630

---

## Importing the CS 1000 Subscriber Manager user data to System Manager

### Before you begin

- Prepare the CS 1000 Subscriber Manager user data for import to System Manager.
- Ensure that the firewall is stopped on the CS 1000 Release 7.x server to gain access to System Manager UPM LDAP.

### Procedure

1. Log on to the Web console of System Manager Release 6.2 or later.
2. Perform the LDAP synchronization as outlined in Importing the Subscriber Manager user data to User Management.

For the directory parameters that you must use, see Subscriber Manager datasource parameters and attributes.

#### Related links

[Importing the Subscriber Manager user data to User Management](#) on page 631

[Subscriber Manager datasource parameters and attributes](#) on page 633

---

## Exporting the CS 1000 user data and creating the user profile

To complete the import job of user data from CS 1000 Subscriber Manager:

### Procedure

Perform the same procedure as System Manager Release 6.1 Exporting the user data and creating the user profile.

#### Related links

[Exporting the user data and creating the user profile](#) on page 634

---

## Preparing the CS 1000 Subscriber Manager user data for import to System Manager

This method uses the CND or LDIF output to capture the CS 1000 Subscriber Manager user data that you later import to User Management in System Manager.

Perform this procedure on System Manager Release 6.2 or later.

### Procedure

1. Log in to the primary CS 1000 UCM server command line using one of the following user names:
  - For CS 1000 Release 7.5 systems, admin2
  - For CS 1000 Release 7.0 and later systems, nortel
2. On the CS 1000 Release 7.x UCM server, perform the steps outlined in Preparing the Subscriber Manager user data for import to User Management in System Manager.
3. Change to super user su - root.
4. Type `cd /opt/nortel/cnd`.
5. Type `./cnd.sh stop_service`.
6. Type `./slapcat -f slapd.conf -s ou=subscribers,dc=nortel,dc=com -a objectclass=nortelsubscriber -l subscriberData.ldif`.
7. Type `./cnd.sh start_service`.
8. Using a secure ftp client, connect to the CS 1000 UCM Linux system using the same credentials you used in Step 1.
9. Copy the `/opt/nortel/cnd/subscriberData.ldif` file to your computer.

### Related links

[Preparing the Subscriber Manager user data for import to User Management](#) on page 630

---

## Importing the CS 1000 UCM Subscriber Manager user data to System Manager

### Before you begin

Prepare the CS 1000 Release 7.x Subscriber Manager user data for import to System Manager User Management.

### Procedure

1. Using a secure ftp client, connect to the System Manager server using admin.
2. Copy the `subscriberData.ldif` file to the `/home/admin` directory on System Manager.
3. Log on to System Manager server using the command line interface.
4. Change to the super user su - root.
5. Type `cd /opt/nortel/cnd`.
6. Type `mv /home/admin/subscriberData.ldif`.



7. Type `./cnd.sh stop_service`.
8. Type `./slapadd -f slapd.conf -l subscriberData.ldif -c`.
9. Type `./cnd.sh start_service`.
10. Perform the LDAP synchronization procedure as outlined in Importing the Subscriber Manager user data to System Manager.

 **Note:**

Ensure that the **Host** field in the **Directory Parameter** area displays localhost.

#### Related links

[Importing the Subscriber Manager user data to User Management](#) on page 631

[Subscriber Manager datasource parameters and attributes](#) on page 633

---

## Exporting the CS 1000 user data and creating the user profile

To complete the import job of user data from CS 1000 Subscriber Manager:

### Procedure

Perform the same procedure as System Manager Release 6.1 Exporting the user data and creating the user profile.

#### Related links

[Exporting the user data and creating the user profile](#) on page 634

---

## Managing messaging

---

### Messaging Class Of Service

A Class Of Service (COS) is a set of messaging capabilities that you define and assign to subscribers. The Class Of Service page lists the current name and number of the different Classes Of Service. You can only view the COS names and numbers on this screen; you cannot use this screen to change the COS names or numbers.

---

### Viewing Class Of Service

#### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. Click **Class Of Service** in the left navigation pane.

3. Choose one or more messaging systems from the Messaging Systems list.
4. Click **Show List**.
5. Click the respective column heading to sort the Class Of Service by **Name** in alphabetical order or by **Class No.** in numeric order.

This is a read-only list.

---

## Class of Service List field descriptions

| Name                    | Description                                                    |
|-------------------------|----------------------------------------------------------------|
| <b>Class No</b>         | The number of each class of service.                           |
| <b>Name</b>             | The name of the class of service.                              |
| <b>Last Modified</b>    | The time and date when the class of service was last modified. |
| <b>Messaging System</b> | The type of messaging system.                                  |

---

## Messaging

### Subscriber Management

With System Manager, you can perform messaging system administration activities, such as add, view, edit, and delete subscribers. You can also administer mailboxes, and modify mailbox settings for a messaging system.

System Manager supports:

- Communication Manager 5.0 and later and
- Avaya Aura® Messaging 6.0 and later

### Adding a subscriber

#### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select one or more messaging systems from the list of Messaging Systems.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions**, and **Miscellaneous** sections.
7. Complete the **Add Subscriber** page and click **Commit** to add the subscriber.

 **Note:**

If you select more than one Messaging or Modular Messaging from the list of messaging systems, and then click **New**, the system displays the Add Subscriber page with the first Messaging or Modular Messaging in context.

## Editing a subscriber

### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. From the Subscriber List, choose the subscriber you want to edit.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields in the **Edit Subscriber** page.
8. Click **Commit** to save the changes.

## Viewing a subscriber

### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to view from the Subscriber List.
6. Click **View**.

 **Note:**

You cannot edit any field on the View Subscriber page.

## Deleting a subscriber

### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Select the subscriber you want to delete from the Subscriber List.
6. Click **Delete**.

The system displays a confirmation page for deleting the subscriber.

7. Confirm to delete the subscriber or subscribers.

 **Note:**

You cannot delete a subscriber associated with a user through mailbox management. You can delete the user associated subscribers only through User Profile Management.

## Subscriber list

The subscriber list displays all subscribers in a messaging version, such as Messaging, Communication Manager Messaging, or Modular Messaging. You can apply filter to each column in the subscriber list. You can also sort subscribers according to each of the column in the subscriber list. You must refresh the page to view the information that is updated after the last synchronization.

| Name                    | Description                                                       |
|-------------------------|-------------------------------------------------------------------|
| <b>Name</b>             | The name of the subscriber.                                       |
| <b>Mailbox Number</b>   | The mailbox number of the subscriber.                             |
| <b>Email Handle</b>     | The email handle of the subscriber.                               |
| <b>Telephone Number</b> | The telephone number of the mailbox.                              |
| <b>Last Modified</b>    | The time and date when the subscriber details were last modified. |
| <b>User</b>             | The name of the user to which the subscriber is associated.       |
| <b>System</b>           | The messaging system of the subscriber.                           |

## Filtering subscribers

### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. Click **Subscriber** in the left navigation pane.
3. Select a messaging system from the list of Messaging Systems.
4. Click **Show List**.
5. Click the **Filter: Enable** option in the Subscriber List.
6. Filter the subscribers according to one or multiple columns.
7. Click **Apply**.

To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

 **Note:**

The table displays only those subscribers that match the filter criteria.

## Subscribers (Avaya Aura® Messaging) field descriptions

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>           | The name of the messaging system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Template</b>         | The messaging template of a subscriber template.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Last Name</b>        | The last name of the subscriber.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>First Name</b>       | The first name of the subscriber.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Mailbox Number</b>   | <p>The full mailbox number of a subscriber, including the site group and site identifiers, and the short mailbox number. Subscribers use mailbox numbers to log on to their respective mailbox. For a PBX subscriber, the mailbox number ranges from 3 to 10 digits in length. Other local subscribers use this field to address messages to the PBX subscriber. For a Multisite system subscriber, the mailbox number is up to 50 digits in length.</p> <p>Ensure that the mailbox number is:</p> <ul style="list-style-type: none"> <li>• Within the range of mailbox numbers assigned to your system.</li> <li>• Unassigned to another local subscriber.</li> <li>• A valid length on the local computer.</li> </ul> <p>This is a mandatory field on the Add Subscriber pages for all types of messaging systems.</p> |
| <b>Password</b>         | <p>The default password the subscriber must use to log in to the mailbox.</p> <p>The password can be from 3 to 15 digits and adhere to system policies set on the Avaya Aura® Messaging server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Save as Template</b> | Saves your current settings as a template.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### Basic Information

| Name                         | Description                                                                                                                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Class Of Service Name</b> | <p>The name of the class of service (CoS) for this subscriber.</p> <p>CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.</p>           |
| <b>Community ID</b>          | <p>The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.</p>                                                                                      |
| <b>Numeric Address</b>       | <p>The unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.</p>                                                                                                                       |
| <b>Time zone</b>             | <p>The time zone for Avaya Aura® Messaging time subscribers.</p> <p>The value must be in the standardized name format, America/Phoenix. Otherwise, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.</p> |

*Table continues...*

| Name                 | Description                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PBX Extension</b> | The primary telephone extension of the subscriber. For a Multisite system subscriber, this number is up to 50 digits in length.                             |
| <b>Site</b>          | The name of the site. Avaya Aura® Messaging includes a site named <b>Default</b> . Change the default name when you set site properties for the first time. |

### Subscriber Directory

| Field                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Email Handle</b>                        | The name that the system displays before the computer name and domain in the subscriber's email address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Telephone Number</b>                    | The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses (()) and ().                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Common Name</b>                         | The display name of the subscriber in address book listings, such as those for email client applications. The name can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>ASCII version of name</b>               | If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Pronounceable Name</b>                  | <p>The pronounceable name of the user.</p> <p>The name of a user, info mailbox, or distribution list might not follow the pronunciation rules of the primary language for your system. To increase the likelihood of the Speech Recognition feature recognizing the name, spell the name as you would pronounce the name.</p> <p>For example, if the primary language of your system is English, spell Dan DuBois as Dan Doobwah. You can enter an alternative name for the user. For example, William Bell might also be known as Bill Bell. If you enter William in the First name field, Bell in the Last name field, and Bill Bell in the Pronounceable name field, the speech engine recognizes both William Bell and Bill Bell.</p> |
| <b>Include in Auto Attendant directory</b> | The option to add the messaging system to the auto attendant directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Subscriber Security

| Name                   | Description                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Expire Password</b> | <p>An option to set the password expiry. The options are:</p> <ul style="list-style-type: none"> <li>• <b>yes</b>: for password to expire</li> <li>• <b>no</b>: if you do not want your password to expire</li> </ul> |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Is Mailbox Locked?</b> | <p>The option to lock your mailbox. A subscriber mailbox can get locked after two unsuccessful login attempts. The options are:</p> <ul style="list-style-type: none"> <li>• <b>no</b>: To unlock your mailbox</li> <li>• <b>yes</b>: To lock your mailbox and prevent access to it</li> </ul> |

## Mailbox Features

| Name                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personal Operator Mailbox</b>  | The mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber greeting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Personal Operator Schedule</b> | The option to specify when to route calls to the backup operator mailbox. The default value is <b>Always Active</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>TUI Message Order</b>          | <p>The order in which the subscriber hears the voice messages. The options are:</p> <ul style="list-style-type: none"> <li>• <b>urgent first then newest</b>: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• <b>oldest messages first</b>: to direct the system to play messages in the order they were received.</li> <li>• <b>urgent first then oldest</b>: to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</li> <li>• <b>newest messages first</b>: to direct the system to play messages in the reverse order of how they were received.</li> </ul> |
| <b>Intercom Paging</b>            | <p>The intercom paging settings for a subscriber. The options are:</p> <ul style="list-style-type: none"> <li>• <b>paging is off</b>: Disables intercom paging for this subscriber.</li> <li>• <b>paging is manual</b>: Callers can page the subscriber with Subscriber Options or TUI if the subscriber can modify.</li> <li>• <b>paging is automatic</b>: Callers automatically page the subscriber with TUI.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                          |

*Table continues...*

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VoiceMail Enabled</b> | <p>The option to specify if a subscriber can receive messages, email messages, and call-answer messages from other subscribers. The options are:</p> <ul style="list-style-type: none"> <li>• <b>yes</b>: To create, forward, and receive messages.</li> <li>• <b>no</b>: To prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.</li> </ul> |
| <b>MWI enabled</b>       | <p>The option to enable the message waiting indicator (MWI) light feature. The options are:</p> <ul style="list-style-type: none"> <li>• <b>No</b>: The user has a voice mailbox only.</li> <li>• <b>ByCOS</b>: CoS controls how the system enables MWI. The <b>MWI enabled</b> field overrides the MWI setting defined by the CoS to which the user is associated.</li> </ul>                                                                                                                                                             |

## Secondary Extensions

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secondary Extension</b> | <p>One or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.</p> <p>For Avaya Aura® Messaging 6.3, you can add a maximum eight secondary extensions.</p> |

## Miscellaneous

| Field                  | Description                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Miscellaneous 1</b> | Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Miscellaneous 2</b> | Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Miscellaneous 3</b> | Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Miscellaneous 4</b> | Useful information about a subscriber template. The messaging system does not use this information. Entries in this field are for convenience and are not used by the messaging system. |



| Button                | Description                    |
|-----------------------|--------------------------------|
| <b>Commit</b>         | Saves all the changes.         |
| <b>Edit</b>           | Allows you to edit the fields. |
| <b>Reset or Clear</b> | Clears all changes.            |
| <b>Cancel</b>         | Returns to the previous page.  |

# Chapter 10: Managing Communication Manager

---

## System Manager Communication Manager capabilities

System Manager provides a common, central administration of some IP Telephony products. This helps you to consolidate the key capabilities of the current suite of Integrated Management administration products with other Avaya Management tools on a common software platform. System Manager helps you administer Avaya Aura® Communication Manager, Communication Manager Messaging, Modular Messaging, Avaya Aura® Messaging. Some features of System Manager include:

- Endpoint management
- Template management
- Mailbox management
- Inventory management
- Element cut through to native administration screens

### Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. From System Manager, you can add, edit, view, or delete the objects through **Communication Manager**.

### Endpoint management

Using endpoint management, you can create and manage endpoint objects, and add, change, remove, and view the endpoint data.

### Templates

Using Templates, you can specify specific parameters of an endpoint or a subscriber once and then reuse the template for subsequent add endpoint or subscriber tasks. You can use default templates or add your own custom templates.

There are two categories of templates: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates at any time.

### Subscriber management

Using Subscriber Management, you can manage, add, change, remove, and view subscriber data. Subscriber management supports Avaya Aura® Messaging, Communication Manager Messaging, and Messaging objects.

With System Manager Communication Manager capabilities, you can:

- Add Communication Manager for endpoints and Modular Messaging for subscribers to the list of managed elements.
- Create templates to simplify endpoint and subscriber management.
- Administer endpoints, subscribers, and create user profiles with communication profiles.
- Associate user profiles with the required endpoints and subscribers.

---

## Configuring Communication Manager user profile settings

Some Communication Manager capabilities depend on the license file available with the customers. For a successful functioning of Communication Manager capabilities, ensure that the following settings are in place:

### Procedure

1. Log in to Communication Manager SAT as a customer super-user.
2. Execute the `display system-parameters customer-options` command.
3. On Page 5, ensure that **Station and Trunk MSP?** is set to **y**.
4. Execute the `duplicate user-profile18` command.
5. On Page 1, perform the following:
  - a. Enter a new profile number. The profile number can range from 20 to 69.
  - b. Set **Shell Access** to **y**.
6. On Page 31, set **station M** to **wm**.
7. Save the user profile settings.
8. Exit Communication Manager SAT.
9. Open Communication Manager shell and perform the following to create a new user and assign password to the new user:
  - a. To create a new user, use the `cmuseradd <type> [-C profile] <login name>` command  
 where,
    - `<type>` is the super-user.
    - `profile` is the profile number created in Step 5.
    - `<login name>` is the user login name.
 For example, `cmuseradd super-user -C 20 iptuser`.
  - b. To assign password to the new user, use the command `cmpasswd <login name>`

where, *<login name>* is the login name in step 9a. For example, `cmpasswd`  
`iptuser`.

 **Note:**

You can also execute Step 9 from the **Administrator Accounts** Web page in Communication Manager SMI. The navigation path for **Administrator Accounts** Web page in Communication Manager SMI is **Administration > Server Maintenance > Security > Administrator Accounts**.

---

## Editing the Select All attribute in a table

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. Click **Settings > Communication System Management > Configuration**.
3. On the View Profile: Configuration page, edit the value of the **Select All** attribute.

This setting affects all the tables in the user interface.

The default value for the **Select All** attribute is 1000. You can increase this value up to 5000.

---

## Search component for Communication Manager objects

System Manager supports data and link search for certain Communication Manager objects. Use the search bar on the Communication Manager objects list page for the following Communication Manager objects:

- Endpoints
- Agents
- Vector Directory Number (VDN)
- Vector
- Vector Routing Table (VRT)
- Announcement
- Audio Group
- Hunt Group
- Off PBX Endpoint Mapping
- Data Module

- Communication System
- Trunk Group
- Signaling Groups

Link based search: When you hover your mouse on the search bar, the system lists the Communication Manager objects that support search. Click a Communication Manager object to go to the relevant page directly. For example, if you click Hunt Group from the search bar, you can directly view the Hunt Group page.

Data search: Free text search and specific search are both supported in the search feature. If you type `Endpoints 100`, the system displays the endpoint with the extension 100. When you hover your mouse on this extension, a pop up window appears by the side. From this window, you can view certain details of the endpoint and directly go to the view, edit, and delete pages for the endpoint.

If you type the name of a Communication Manager object followed by space, the system lists all the searchable fields for the particular CM object. You can click a particular field and use the search option for that field.

The following table lists the fields that are searchable for the supported Communication Manager objects:

| Communication Manager object | Searchable fields                                                                                                                                              | Supported Actions  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| Endpoint                     | Name, Extension, Port, Set Type, TN, Location, IP soft phone, COS, COR, User, Communication Manager name, Emergency Location Extension, Message Lamp Extension | View, Edit, Delete |
| Agent                        | Extension, Name, AAS, Call Handling Preference, COR, User, Coverage Path, Communication Manager name                                                           | View, Edit, Delete |
| VDN                          | Extension, Name, Destination, Allow VDN Override, Attendant, Vectoring, Meet-me Conferencing, COR, TN, Communication Manager name                              | View, Edit, Delete |
| Vector                       | Number, Name, Multimedia Attendant, Vectoring, Meet-me Conf, Communication Manager name                                                                        | View, Edit         |
| VRT                          | Number, Name, Sort, Communication Manager name                                                                                                                 | View, Edit, Delete |
| Announcement                 | Name, Extension, Group/Board, Type, Protected, Rate, COR, TN, Queue Size, Communication Manager name                                                           | View, Edit, Delete |
| Audio Group                  | Group Number, Group Name, Communication Manager name                                                                                                           | View, Edit, Delete |

*Table continues...*

| Communication Manager object | Searchable fields                                                                 | Supported Actions  |
|------------------------------|-----------------------------------------------------------------------------------|--------------------|
| Hunt Group                   | Group Number, Group Name, Group Extension, Group Type, Communication Manager name | View, Edit, Delete |

 **Note:**

You must have at least View permission for a Communication Manager object to use the search component for that Communication Manager object.

When you search a Communication Manager object, the system also displays the search results for other Communication Manager objects which support the search feature.

---

## Managing Communication Manager objects

---

### Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. Through **Communication Manager** you can directly add, edit, view, or delete the Communication Manager objects.

 **Note:**

To manage the Communication Manager objects not identified here, access the Communication Manager Element Cut-Through which provides an enhanced System Access Terminal (SAT) interface. To launch Element Cut-Through, click **Inventory > Synchronization > Communication System**.

The Communication Manager objects you can administer through System Manager are:

| Group       | Communication Manager objects                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Call Center | Agents<br>Announcements<br>Audio Group<br>Best Service Routing<br>Holiday Tables<br>Variables<br>Vector<br>Vector Directory Number<br>Vector Routing Table<br>Service Hours Tables |
| Coverage    | Coverage Answer Group<br>Coverage Path<br>Coverage Remote<br>Coverage Time of Day                                                                                                  |
| Endpoints   | Alias Endpoint<br>Intra Switch CDR<br>Manage Endpoints<br>Off PBX Endpoint Mapping<br>Site Data<br>Xmobile Configuration                                                           |
| Groups      | Group Page<br>Hunt Group<br>Intercom Group<br>Pickup Group<br>Terminating Extension Group                                                                                          |

*Table continues...*

| Group      | Communication Manager objects                                                                                                                                                                                                                                                                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network    | Automatic Alternate Routing Analysis<br>Automatic Alternate Routing Digit Conversion<br>Automatic Route Selection Analysis<br>Automatic Route Selection Digit Conversion<br>Automatic Route Selection Toll<br>Cluster Session Manager<br>Data Modules<br>IP Interfaces<br>IP Network Regions<br>IP Network Maps<br>Node Names<br>Route Pattern<br>Signaling Groups<br>Trunk Group |
| Parameters | System Parameters - CDR Options<br>System Parameters - Customer Options<br>System Parameters - Features<br>System Parameters - Security<br>System Parameters - Special Applications                                                                                                                                                                                               |
| System     | Abbreviated Dialing Enhanced<br>Abbreviated Dialing Group<br>Abbreviated Dialing Personal<br>Authorization Code<br>Class of Restriction<br>Class of Service<br>Class of Service Group<br>Dialplan Analysis<br>Dialplan Parameters<br>Feature Access Codes<br>Locations<br>Uniform Dial Plan<br>Uniform Dial Plan Group<br>Tenant                                                  |



 **Note:**

You cannot add, edit, or delete Audio Groups, Announcements, Subscribers, and Class of Service objects through Element Cut Through.

## Export function of Communication Manager objects

When you export the selected object or all objects, System Manager exports the objects in an excel sheet.

Note the following points:

- The Excel sheet has hyperlink limit of 65530. If the hyperlinks in the exported excel sheet exceeds from the provided limit, System Manager stops adding new hyperlinks. To maintain consistency, the font size is same for the text where hyperlink is applicable and even if hyperlink is not added.
- The Excel sheet has row limit of 1048576. If this limit is reached while exporting data on any sheet, System Manager creates a new file and continues exporting the data in the new Excel sheet. Once all data is exported, all the excel files are merged in a zip. So, if there are more than one Excel files then the Export Job list provides link to the zip file. Otherwise, System Manager provides the direct excel download.

### Related links

[Adding Communication Manager objects](#) on page 655

[Editing Communication Manager objects](#) on page 656

[Viewing Communication Manager objects](#) on page 656

[Deleting Communication Manager objects](#) on page 656

[Filtering Communication Manager objects](#) on page 657

## Adding Communication Manager objects

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Select the Communication Manager object.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Select the Communication Manager again from the list of Communication Managers.

 **Note:**

Enter the qualifier number in the **Enter Qualifier** field, if applicable.

7. Click **Add**.

The system displays the Element Cut Through screen where you can enter the attributes of the Communication Manager object you want to add.

8. Click **Enter** to add the Communication Manager object.

To return to the Communication Manager screen, click **Cancel**.

## Editing Communication Manager objects

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Select the Communication Manager object.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the group list, select the device you want to edit.
6. Click **Edit**.

The system displays the Element Cut Through screen where you can edit the attributes of the device you have chosen.

7. To save the changes and go back to the Communication Manager screen, click **Enter**.

To undo the changes and return to the Communication Manager screen, click **Cancel**.

## Viewing Communication Manager objects

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Select the Communication Manager object.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the group list, select the object you want to view.
6. Click **View**.

You can view the attributes of the object you have selected in the Element Cut Through screen.

7. To return to the Communication Manager screen, click **Cancel**.

## Deleting Communication Manager objects

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Select the Communication Manager object.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. Select the objects you want to delete from this group.
6. Click **Delete**.
7. Confirm to delete the Communication Manager objects.

## Filtering Communication Manager objects

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Select the Communication Manager object.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the group list.
6. Filter the Communication Manager objects according to one or multiple columns.
7. Click **Apply**.

To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

#### **Note:**

The table displays only those devices that match the filter criteria.

## Changing to classic view

The System Manager Web interface of Communication Manager objects support two types of views: classic and enhanced. Enhanced view is the default setting, where you can execute tasks on the Web interface. In the classic view, the system directs you to Element Cut Through screen for executing the tasks.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Select the Communication Manager object you want to manage.
3. By default, the system displays the Web page for the Communication Manager object in enhanced view. To change to classic view, click the **Switch to Classic View** link on the upper-right of the interface.
4. To return to the default view, click the **Switch to Enhanced View** link.

---

## Agents

### Agents

Use the Agents capability to manage agent login IDs and skill assignments in an Expert Agent Selection (EAS) environment. If skills are added or changed, agents must log out and then log in again before the changes are effective.

### Agents List

Agents List displays all the agents under the Communication Manager you select. You can perform an advanced search on this list using the search criteria. You can also apply filters and sort each column in the Agents List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                            | Description                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------|
| <b>LoginID</b>                  | The identifier for the Logical Agent as entered in the command line.                              |
| <b>Agent Name</b>               | The 27-character string name of the agent. Any alphanumeric character is valid. Default is blank. |
| <b>Direct Agent Skill</b>       | The number of the skill used to handle Direct Agent calls.                                        |
| <b>Call Handling Preference</b> | The call that an agent receives the next when calls are in queue.                                 |
| <b>COR</b>                      | The Class of Restriction associated with the agent.                                               |
| <b>System</b>                   | The name of the Communication Manager associated with the agents.                                 |

### Adding an agent

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. From **Template**, select the template.
7. In **Login ID**, perform one of the following:
  - Type the extension number.
  - Click the **Display Extension Ranges** link to select the extension number from the available extension ranges.
8. Complete the New Agent page and click **Commit**.

**Related links**

[Agents field descriptions](#) on page 663

**Viewing agent data****Procedure**

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agent whose data you want to view.
6. Click **View**.

**Related links**

[Agents field descriptions](#) on page 663

**Editing agent data****Procedure**

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Agents List, select the agent whose properties you want to edit.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields on the **Edit Agent** page.
8. Click **Commit** to save the changes.

**Related links**

[Agents field descriptions](#) on page 663

**Deleting agents****Procedure**

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. From the Agents List, select the agents you want to delete.
6. Click **Delete**.
7. Confirm to delete the agents.

#### Related links

[Agents field descriptions](#) on page 663

## Adding agents in bulk

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Bulk Add Agents**.
6. Complete the **Bulk Add Agents** page and click **Now**.

The **Agent Name Prefix** field displays the common prefix which appears for all the agents you bulk add. You can enter any prefix name of your choice in this field.

#### **Note:**

With Multi Tenancy, when you add the agents, the **Tenant Number** field is auto populated according to the Site you select.

Fields like **COR** are validated with the tenant permissions when you add the agents.

#### Related links

[Agents field descriptions](#) on page 663

## Editing agent data in bulk

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Bulk Edit Agents**.
6. Complete the **Bulk Edit Agents** page and click **Now**.

The **Agent Name Prefix** field displays the common prefix which appears for all the agents you bulk add. You can enter any prefix name of your choice in this field.

**Related links**

[Agents field descriptions](#) on page 663

**Deleting agents in bulk****Procedure**

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Bulk Delete Agents**.
6. Perform one of the following actions:
  - Select the agents you want to delete in bulk from the **Current Agent Extensions** field.
  - Type the agent extensions you want to bulk delete in the **Enter Extensions** field.
7. Click **Continue**.
8. On the Bulk Delete Agents Confirmation page, click **Now**.  
Click **Schedule** to schedule the bulk delete job at a later time.

 **Note:**

You cannot delete agent associated extensions.

**Exporting selected agent****Procedure**

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the **Agent List**, select the agent you want to export.
6. Click **More Actions > Export Selected Agents**.  
The system displays the **Export AgentLoginIds** page.
7. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
8. Click **Export**.

System Manager displays the status of the exported job in the **Status** column of the Export Jobs List section.

## Exporting all agents

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Export All Agents**.

The system displays the **Export All AgentLoginIds** page.

6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

System Manager displays the status of the exported job in the **Status** column of the Export Jobs List section.

## Importing agents

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Import Agents**.

The system displays the **Import CM Objects** page.

6. In the **Select a file** field, click **Browse** to select the required excel file.
7. In the **Select Error Configuration** field, select one of the following.

The default option is **Continue processing other records**.

- **Abort on first error**
- **Continue processing other records**

8. In the **If a matching record already exists** field, select one of the following:

The default option is **Skip**.

- **Skip**
- **Merge**
- **Delete**

9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.



10. Click **Import**.

System Manager displays the status of the imported job in the **Status** column of the Import Jobs List section.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Agents**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

System Manager saves the file on your local computer.

## Agents field descriptions

If you change the value of the fields from the systemparameters features screen of Communication Manager, agents must log out and log back in for the change to be reflected.

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                    | The Communication Manager system in which you have added the agent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Login ID</b>                  | The identifier for the Logical Agent as entered in the command line. This is a display-only field.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Template</b>                  | The agent template.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Name</b>                      | The 27-character string name of the agent. Any alphanumeric character is valid. By default, this field is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Attribute</b>                 | The agent attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>AAS</b>                       | <p>The option to use this extension as a port for an Auto Available Split/Skill. By default, this check box is clear. This option is intended for communication server adjunct equipment ports only, not human agents.</p> <p> <b>Important:</b></p> <p>When you enter <i>y</i> in the AAS field, it clears the password and requires execution of the <b>remove agent-loginid</b> command. To set AAS to <i>n</i>, remove this logical agent, and add it again.</p> |
| <b>ACW Agent Considered Idle</b> | The option to count After Call Work (ACW) as idle time. The valid entries are <b>System</b> , <b>Yes</b> , and <b>No</b> . Select <b>Yes</b> to include ACW agents in the Most-Idle Agent queue. Select <b>No</b> to exclude ACW agents from the queue.                                                                                                                                                                                                                                                                                                 |

*Table continues...*

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AUDIX</b>                           | <p>The option to use this extension as a port for AUDIX. By default, this check box is clear.</p> <p> <b>Note:</b></p> <p>Both AAS and AUDIX fields cannot be <i>y</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>AUDIX Name for Messaging</b>        | <p>The name of the AUDIX Messaging System.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• The messaging system used for LWC Reception.</li> <li>• The messaging system that provides coverage for this Agent LoginID.</li> <li>• Blank, the default value.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Auto Answer</b>                     | <p>When using EAS, the auto answer setting of the agent applies to the endpoint where the agent logs in. If the auto answer setting for that endpoint is different, the agent setting overrides the endpoint setting. One of the following is a valid entry:</p> <ul style="list-style-type: none"> <li>• <b>All</b>. Immediately sends all ACD and non-ACD calls to the agent. The endpoint is also given a single ring while a non-ACD call is connected. You can use the ringer-off button to prevent the ring when the feature-related system parameter, <b>Allow Ringer-off with Auto-Answer</b>, is set to <i>y</i>.</li> <li>• <b>acd</b>. Only ACD split /skill calls and direct agent calls go to auto answer. If this field is set to <b>acd</b>, non-ACD calls terminated to the agent ring audibly.</li> <li>• <b>none</b>. All calls terminated to this agent receive an audible ringing. This is the default setting.</li> <li>• <b>station</b>. Auto answer for the agent is controlled by the auto answer field on the Endpoint screen.</li> </ul> |
| <b>Aux Agent Considered Idle (MIA)</b> | <p>To include agents who are in the AUX mode in the Most Idle Agent (MIA) queue. Communication Manager counts the time in AUX as idle time.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>System</b>: Communication Manager uses the system-wide field settings.</li> <li>• <b>Yes</b>: Communication Manager keeps or places agents in the MIA queue while they are in AUX work.</li> <li>• <b>No</b>: Communication Manager excludes AUX agents from the MIA queue while they are in AUX work. The <b>No</b> value matches the legacy Communication Manager functionality.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

*Table continues...*

| Name                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aux Work Reason Code Type</b>         | <p>Determines how agents enter reason codes when entering AUX work. One of the following is a valid entry:</p> <ul style="list-style-type: none"> <li>• <b>system.</b> Settings assigned on the Feature Related System Parameters screen apply. This is the default setting.</li> <li>• <b>none.</b> You do not want an agent to enter a reason code when entering AUX work.</li> <li>• <b>requested.</b> You want an agent to enter a reason code when entering AUX mode but do not want to force the agent to do so. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to <i>y</i>.</li> <li>• <b>forced.</b> You want to force an agent to enter a reason code when entering AUX mode. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to <i>y</i>.</li> </ul> |
| <b>Call Handling Preference</b>          | <p>Determines which call an agent receives next when calls are in queue. When calls are in queue and an agent becomes available, any of the following entries is valid:</p> <ul style="list-style-type: none"> <li>• <b>skill-level.</b> Delivers the oldest, highest priority calls waiting for the highest-level agent skill.</li> <li>• <b>greatest-need.</b> Delivers the oldest, highest priority calls waiting for any agent skill.</li> <li>• <b>percent-allocation.</b> Delivers a call from the skill that will otherwise deviate most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software.</li> </ul> <p>For more information, see <i>Avaya Business Advocate User Guide</i>.</p>                                                                                                                                  |
| <b>Check skill TNs to match agent TN</b> | The skill tenant number to match the tenant number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>COR</b>                               | The Class Of Restriction (COR) for the agent. Valid entries range from <b>0</b> to <b>995</b> . The default entry is <b>1</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Coverage Path</b>                     | The coverage path number used by calls to the LoginID. A valid entry is a path number from <b>1</b> to <b>999</b> , time of day table <b>t1</b> to <b>t999</b> , or blank by default. Coverage path is used when the agent is logged out, busy, or does not answer calls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Direct Agent Calls First</b>          | The option to direct agent calls to override the percent-allocation call selection method and be delivered before other ACD calls. Clear the check box if you want to treat direct agent calls as other ACD calls. This field replaces the <b>Service Objective</b> field when percent-allocation is entered in the Call Handling Preference field. For more information, see <i>Avaya Business Advocate User Guide</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Direct Agent Skill</b>                | The number of the skill used to handle Direct Agent calls. A valid entry can range from <b>1</b> to <b>2000</b> , or blank. The default setting is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Forced Agent Logout Time</b>           | Enables the Forced Agent Logout by Clock Time feature by administering a time of day to automatically log out agents using an hour and minute field. A valid entry for the hour field ranges from <b>01</b> to <b>23</b> . A valid entry for the minute field is <b>00</b> , <b>15</b> , <b>30</b> , or <b>45</b> . The default is blank (not administered). Examples are: 15:00, 18:15, 20:30, 23:45.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hears Service Observing Tone</b>       | When you enable the <b>(SA8569) - No Service Observing Tone Heard by Agent</b> field on the Special Application form, the system enables the <b>Hears Service Observing Tone</b> field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Include Tenant Calling Permissions</b> | The tenant calling permissions.<br><br> <b>Note:</b><br>To enable this feature you must first select <b>Check skill TNs to match agent TN</b> checkbox.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Local Call Preference</b>              | The option to administer Local Preference Distribution to handle agent-surplus conditions, call-surplus conditions, or both. Use this field to administer call-surplus conditions. To set up an algorithm for agent-surplus conditions, set the Local Agent Preference field on the Hunt Group screen. You can select this check box only if the Call Center Release field is set to 3.0 or later and the Multiple Locations customer option is active.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>LoginID for ISDN/SIP Display</b>       | Use to include the <b>Agent LoginID CPN and Name</b> field in ISDN and SIP messaging over network facilities. By default, the check box is clear, indicating that the physical endpoint extension CPN and Name is sent. If you set the <b>Send Name</b> to n or r (restricted) on the ISDN Trunk Group screen, the calling party name and number is sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Logout Reason Code Type</b>            | Determines how agents enter reason codes. One of the following is a valid entry: <ul style="list-style-type: none"> <li>• <b>System.</b> Settings assigned on the Feature Related System Parameters screen apply. This is the default entry.</li> <li>• <b>Requested.</b> You want an agent to enter a reason code when logging out but do not want to force the agent to do this. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to <u>y</u>.</li> <li>• <b>Forced.</b> You want to force an agent to enter a reason code when logging out. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to <u>y</u>.</li> <li>• <b>None.</b> You do not want an agent to enter a reason code when logging out.</li> </ul> |
| <b>LWC Log External Calls</b>             | Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table continues...

| Name                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LWC Reception</b>                                 | <p>Indicates whether the terminal can receive Leave Word Calling (LWC) messages. One of the following is a valid entry:</p> <ul style="list-style-type: none"> <li>• <b>audix</b></li> <li>• <b>msa-spe</b>. This is the default entry.</li> <li>• <b>none</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Maximum time agent in ACW before logout (Sec)</b> | <p>Sets the maximum time the agent can be in ACW on a per agent basis. One of the following is a valid entry:</p> <ul style="list-style-type: none"> <li>• <b>system</b>. This is the default entry. Settings assigned on the Feature Related System Parameters screen apply.</li> <li>• <b>none</b>. ACW timeout does not apply to this agent.</li> <li>• <b>30-9999 sec</b>. Indicates a specific timeout period. This setting will take precedence over the system setting for maximum time in ACW.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>MIA Across Skills</b>                             | <p>To remove an agent from the MIA queue for all splits or skills that the agent is available in when the agent answers a call from any assigned splits or skills.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>System</b></li> <li>• <b>Yes</b></li> <li>• <b>No</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Multibyte Language</b>                            | <p>When you configure agent information, if the localized display name contains multiscrypt language characters, you must set the then multibyte language or locale. You can set the locale using the <b>Multibyte Language</b> field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>MWI Served User Type</b>                          | <p>This field is available for Communication Manager Release 7.1.3.6 and Release 8.1.2 and later. However, System Manager Release 8.1.2 displays this field on the Agent add/edit page if you select Communication Manager Release 7.1 and later. If the <b>MWI Served User Type</b> field is administered on System Manager and Communication Manager Release does not have the value in this field, you can create Agent but the system operations will be unaffected.</p> <p>Controls the auditing of a served user's message waiting indicator (MWI).</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>None</b>: The served user's MWI is not audited. The user's MWI is not audited if the user is not served by an fp-mwi, qsig-mwi, or sip-adjunct message center.</li> <li>• <b>fp-mwi</b>: The agent is a served user of an fp-mwi message center.</li> <li>• <b>qsig-mwi</b>: The agent is a served user of a qsig-mwi message center.</li> <li>• <b>sip-adjunct</b>: Use this option to audit the user's MWI.</li> </ul> |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Percent Allocation</b> | The percentage for each of the agent skills if the call handling preference is percent-allocation. a valid entry is a number from <b>1</b> to <b>100</b> for each skill. Entries for all the agent skills together must add up to 100%. Do not use target allocations for reserve skills. Percent Allocation is available as part of the Avaya Business Advocate software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Password</b>           | The password the agent must enter upon login. Displayed only if both the AAS and AUDIX check boxes are clear. A valid entry is a digit ranging from <b>0</b> through <b>9</b> . Enter the minimum number of digits in this field specified by the <b>Minimum Agent-LoginID Password Length</b> field on the Feature-Related System Parameters screen. By default, this field is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Confirm Password</b>   | <p>Confirms the password the agent entered in the Password field during login. Displayed only if both the AAS and the AUDIX check boxes are clear. By default, this field is blank.</p> <p> <b>Note:</b><br/>Values entered in this field are not populated to the screen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Port Extension</b>     | The assigned extension for the AAS or AUDIX port. The values are displayed only if either the AAS or AUDIX check box is selected. This extension cannot be a VDN or an Agent LoginID. By default, this field is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Reserve Level</b>      | <p>The reserve level to be assigned to the agent for the skill with the Business Advocate Service Level Supervisor feature or the type of interruption with the Interruptible AUX Work feature. You can assign a reserve level of 1 or 2 or an interruptible level of a, m, n, or blank for no reserve or interruptible level, where,</p> <ul style="list-style-type: none"> <li>• a is auto-in-interrupt</li> <li>• m is manual-in-interrupt</li> <li>• n is notify-interrupt</li> </ul> <p>Changes to this field take effect the next time the agent logs in. Values of 1 and 2 are allowed only if Business Advocate is enabled. A skill level cannot be assigned with a reserve level setting. Reserve level set to 1 or 2 defines the EWT threshold level for the agent to be added to the assigned skill as a reserve agent. When the EWT for this skill reaches the corresponding threshold set on the Hunt Group screen, this skill gets this skill gets automatically added to the logged in skills of the agents. Agents are delivered calls from this skill until the skill EWT drops below the assigned overload threshold. Use the Interruptible Aux functionality to help meet service level targets by requesting agents who are on break to become available when the service level target is not being met. For more information on Service Level Supervisor, see <i>Avaya Business Advocate User Guide</i>.</p> |

Table continues...

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Service Objective</b> | The option to administer Service Objective. Service Objective is administered on the Hunt Group screen and the agent LoginID screen. This field is displayed only when Call Handling Preference is set to greatest-need or skill-level. The communication server selects calls for agents according to the ratio of Predicted Wait Time (PWT) or Current Wait Time (CWT) and the administered service objective for the skill. Service Objective is part of the Avaya Business Advocate software.                                                                                                                                                    |
| <b>Skill Number</b>      | <p>The Skill Hunt Groups that an agent handles. The same skill cannot be entered twice. You have the following options:</p> <ul style="list-style-type: none"> <li>• If EAS-PHD is not optioned, enter up to four skills.</li> <li>• If EAS-PHD is optioned, enter up to 20 or 60 skills depending on the platform.</li> </ul> <p> <b>Important:</b></p> <p>Assigning a large number of skills to agents can potentially impact system performance. Review system designs with the ATAC when a significant number of agents have more than 20 skills per agent.</p> |
| <b>Skill Level</b>       | A skill level for each of an agent assigned skills. If you specify the EAS-PHD option, 16 priority levels are available. If you do not specify this option, two priority levels are available.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Tenant Number</b>     | <p>The tenant partition number. A valid entry ranges from <b>1</b> to <b>100</b>. The default is <b>1</b>.</p> <p> <b>Note:</b></p> <p>Values entered in this field are not echoed to the screen.</p>                                                                                                                                                                                                                                                                                                                                                             |

| Button                                                                           | Description                                                                                                                                  |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commit</b>                                                                    | Completes the action you initiate.                                                                                                           |
| <b>Schedule</b>                                                                  | Performs the action at the chosen time.                                                                                                      |
| <b>Reset</b>                                                                     | Clears the action and resets the field.                                                                                                      |
| <b>Clear</b>                                                                     | Clears all entries.                                                                                                                          |
| <b>Edit</b>                                                                      | Allows you to edit the fields in the page.                                                                                                   |
| <b>Commit with Auto Logout/Login</b> (applicable only for the Edit Agent page)   | Enabling automatic logout and login after you commit a change. After automatic logout and login, the change you made takes immediate effect. |
| <b>Schedule with Auto Logout/Login</b> (applicable only for the Edit Agent page) | Scheduling automatic logout and login every time you edit an agent property.                                                                 |
| <b>Done</b>                                                                      | Completes your current action and takes you to the subsequent page.                                                                          |
| <b>Cancel</b>                                                                    | Cancels your current action and takes you to the previous page.                                                                              |
| <b>Now</b>                                                                       | Performs the action you initiate real time.                                                                                                  |

---

## Announcements

### What is an announcement?

An announcement is a recorded message that a caller hears while the call is in a queue. An announcement is often used in with music.

Announcements are recorded on:

- Special circuit packs (TN750, TN750B, TN750C, or TN2501AP).
- Disk/Flash Memory as vVAL in H.248 Media Gateways.
- Disk or content store on Avaya Aura® Media Server or also can be sourced from an internet source if using Avaya Aura® MS.

The three types of announcements are:

- Delay announcement: Explains the reason for the delay and encourages the caller to wait
- Forced announcement: Explains an emergency or service problem. Use when you anticipate a large number of calls about a specific issue
- Information announcement: Gives the caller instructions on how to proceed, information about the number called, or information that the caller wants

Announcements are most effective when they are:

- Short, courteous, and to-the-point
- Spaced close together when a caller on hold hears silence
- Spaced farther apart when music or ringing is played on hold
- Played for calls waiting in queue

While scheduling backup or backing up all jobs from the List Announcement page, if the backup size is:

- Greater than 1 GB, the system does not schedule the job and displays an error.
- Less than 1 GB or if system estimates that the backup size is exceeding 1 GB limit while executing the job, the scheduled job fails with error: `Used size has exceeded the maximum allowed size. Consider removing the old backups.`

Music on Hold is a package of professionally-recorded music available from Avaya.

From Release 7.0, with Avaya Aura® Media Server, you can upload up to 10 MB size of .wav files.

### Announcement List

Announcement list displays the property of an announcement. To view the announcement list, on the **Elements** menu, navigate to **Communication Manager > Call Center > Announcements**.



| Name               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | The file name of the audio file. The alphanumeric file name can contain up to 27 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Extension</b>   | The valid extension number for the announcement. Extension numbers might not include punctuation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Group/Board</b> | Indicates whether the announcement's audio file exists on the VAL board. Type the group number in the format gggV9 for media gateway vVAL, where ggg is the gateway number of the media gateway (up to 250).                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Type</b>        | The type of the announcement. Possible values include: <ul style="list-style-type: none"> <li>• <b>Integ-mus.</b> Integrated music type</li> <li>• <b>Integ-rep.</b> Integrated repeating type</li> <li>• <b>Integrated.</b> Stored internally on a special integrated announcement circuit pack. Use this for general announcements and VDN of Origin Announcements.</li> </ul>                                                                                                                                                                                                                                                                                             |
| <b>Protected</b>   | Use this field to set the protection mode for an integrated announcement.<br><br>When you set this field to <b>y</b> , the recording is protected and cannot be deleted or changed through a telephone session or FTP.<br><br>When you set this field to <b>n</b> , you can change or delete the recording if you have the corresponding console permissions.                                                                                                                                                                                                                                                                                                                |
| <b>Rate</b>        | If the VAL board is administered on the circuit packs form, then the system automatically displays 64 (64Kbps) in the <b>Rate</b> field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>COR</b>         | The Class of Restriction associated with this announcement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>TN</b>          | The tenant partition number of the announcement. A valid entry ranges from 1 to 100.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Queue</b>       | The announcement queuing or barge-in. Possible values include: <ul style="list-style-type: none"> <li>• <b>no:</b> Indicates that the announcement does not play if a port is not available. This is the default value.</li> <li>• <b>yes:</b> Indicates that the request queues when all ports on the circuit pack are busy. The announcement plays when a port becomes available. This setting is used in most call center applications.</li> <li>• <b>bargein:</b> Indicates that you can connect callers to the announcement at any time while it is playing. With <b>n</b> or <b>y</b>, the caller is always connected to the beginning of the announcement.</li> </ul> |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Live Stream Source</b> | Indicates if the announcement is played live from an external source or from an audio file.<br><br>After you configure the announcement with Live Stream Source type, play once to ensure that the live streaming feature works correctly.<br><br>When you deactivate the Release 8.1.3 patch, the system runs on Release 8.1.3 system and sets the <b>Live Stream Source</b> feature to <i>n</i> . Therefore, you must install and activate the new Release 8.1.3 patch immediately to prevent the system processes from running on the Release 8.1.3 system. You must also set the value of the <b>Live Stream Source</b> feature to <i>y</i> . |
| <b>Size</b>               | The size of the audio files in kilobytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Timestamp</b>          | The date and time the audio file was created or modified. This changes each time the audio file is put on the VAL board using FTP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>System</b>             | The name of the Communication Manager associated with the announcement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Adding an announcement

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.
6. On the New Announcement page, complete the fields and click **Commit**.

For more information, see “Announcements field descriptions”.

### Related links

[Announcements field descriptions](#) on page 679

## Editing an announcement

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to edit from the Announcement List.

6. Click **Edit** or **View > Edit**.
7. Edit the required fields on the **Edit Announcement** page.
8. Click **Commit** to save the changes.

#### Related links

[Announcements field descriptions](#) on page 679

## Viewing an announcement

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to view.
6. Click **View**.

You can view the properties of the announcement in the **View Announcements** page.

#### Related links

[Announcements field descriptions](#) on page 679

## Deleting an announcement

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcement you want to delete from the Announcement List.
6. Click **Delete**.
7. Confirm to delete the announcements.

## Saving an announcement

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. Select the announcement you want to save from the Announcement List.
6. Click **More Actions** > **Save**.

This action internally edits and updates the announcements in the Communication Manager.

#### Related links

[Announcements field descriptions](#) on page 679

## Backing up announcements

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the announcements you want to backup.
6. Click **More Actions** > **Backup** to back up your announcements.

#### Related links

[Announcements field descriptions](#) on page 679

## Backing up all announcements

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions** > **Backup All** to back up all the announcements.

## Downloading announcements

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Call Center** > **Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. Click **More Actions > Download**.
6. Select the files you want to download from the Backedup Announcements list.
7. Click **Download** to download the backed up announcements.

#### Related links

[Announcements field descriptions](#) on page 679

## Restoring announcements

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Restore**.
6. Select one or more Communication Manager instance from the Communication Manager list.
7. Select the options from the Restore Options section.
8. If you want to restore from client, select the **Restore from Client** check box.
9. Select the announcements you want to restore from the Backedup Announcement List.
10. Click **Restore** to restore your announcement and announcement property files from your application to a VAL/Virtual VAL board you select.

#### Related links

[Announcements field descriptions](#) on page 679

## Restoring all announcements

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Restore All**.

## Moving an announcement

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.

2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Move**.
6. Select the destination where you want to move the announcement.
7. Click **Now** to move the announcement from one VAL board to another within the same voice system.

#### Related links

[Announcements field descriptions](#) on page 679

## Broadcasting announcements

### About this task

You can upload an audio file on multiple media sources using the **Broadcast** operation. The media sources can be Media Servers, Media Gateways, or VAL Board. You can also transfer audio files from one board to the other of the same Communication Manager or boards (VAL Board, Media Gateway, or Media Server) of another Communication Manager.

Uploading audio files to media servers is done using a SOAP request. System Manager uses FTP or SCP for Media Gateway and FTP or SFTP for VAL Board. The transfer protocol for Media Gateway or VAL Board can be configured from File Transfer Settings. FTP is the default protocol for file transfer on VAL Board and Media Gateway.

With Release 8.1.1, you can upload more than one audio file (.wav) with a single click by using the **Browse** option of the **Select Announcement File** field.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Do one of the following:
  - To transfer an audio file from one audio source to another:
    - a. Select the announcement that you want to broadcast from the Announcement list.
    - b. Click **More Actions > Broadcast**.
  - To upload an audio file from your computer and broadcast it to audio sources:
    - a. Click **More Actions > Broadcast**.
    - b. On the Broadcast Announcements page, in **Select Announcement File**, click **Browse**.

- c. In the File Upload dialog box, select one or more audio files from your local computer.

System Manager displays the uploaded audio files (.wav) with file name on the Broadcast Announcements page.

 **Note:**

If you remove one of the uploaded audio files using the browse option, the system removes all the files that were uploaded together.

6. In the Select Destination for Broadcasting Announcements section, select the destination VAL source, which includes media servers too.
7. Do one of the following:
  - Click **Now** to immediately broadcast the announcement files to various VAL boards on voice system or media servers.
  - Click **Schedule** to schedule a broadcast operation later.

On the Job Scheduler page, you can set a later time to broadcast the announcement files to various VAL boards on voice system or media servers.

#### Related links

[Announcements field descriptions](#) on page 679

[Using File Transfer Settings](#) on page 677

[Announcements field descriptions](#) on page 679

## Using File Transfer Settings

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select an announcement from the Announcement List.
6. Click **More Actions > File Transfer Settings**.
7. Select a VAL board from the VAL Board and Media Gateway list.
8. Click **Done**.

#### Related links

[Announcements field descriptions](#) on page 679

## Using List Usage Extension

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.

2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select an announcement from the Announcement List.
6. Click **More Actions > List Usage Extension**.  
You can view the details of the announcement through the List Usage for Extension list.
7. Click **Done**.

#### Related links

[Announcements field descriptions](#) on page 679

## Filtering the Announcements list

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Click **Filter: Enable** in the Announcement list.
4. Filter the list according to one or multiple columns.
5. Click **Apply**.

To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

#### **Note:**

The table displays only those options that match the filter criteria.

## Using Advanced Search

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Announcements**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in Announcement List.
6. In the Criteria section, do the following:
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter the search value in the third field.



If you want to add a search condition, click the plus sign (+) and repeat the substeps listed in Step 5.

If you want to delete a search condition, click the minus sign (-). This button is available if there is more than one search condition.

7. Click **Search**.

## Announcements field descriptions

| Name             | Description                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>    | The name of the Communication Manager associated with the announcement.                                                                                                                                                                                                                                                                                                   |
| <b>Name</b>      | The filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.                                                                                                                                                                                                                                                                         |
| <b>Extension</b> | A valid extension number for the announcement. Extension numbers must not include punctuation.                                                                                                                                                                                                                                                                            |
| <b>Source</b>    | <p>The field that indicates whether the announcement's audio file exists on the VAL board.</p> <ul style="list-style-type: none"> <li>Type the group number in the format gggV9 for media gateway vVAL, where ggg is the gateway number of the media gateway (up to 250).</li> <li>Type the identifier for the Media Server device.</li> </ul>                            |
| <b>Type</b>      | <p>The type of announcement. The options are:</p> <ul style="list-style-type: none"> <li><b>Integ-mus</b>. Integrated music type.</li> <li><b>Integ-rep</b>. Integrated repeating type.</li> <li><b>Integrated</b>. A special integrated announcement circuit pack stored internally. Use this for general announcements and VDN of Origin Announcements.</li> </ul>      |
| <b>Protected</b> | <p>The field to set the protection mode for an integrated announcement. The options are:</p> <p><b>y</b>: The recording is protected, and you cannot delete or change it through a telephone session or FTP.</p> <p><b>n</b>: You can change or delete the recording if you have the corresponding console permissions.</p>                                               |
| <b>Rate</b>      | <p>The recording rate speed for announcements. If the VAL board is administered on the circuit packs form, then 64 (64Kbps) automatically appears in this field.</p> <p> <b>Note:</b></p> <p>The system disables the <b>Rate</b> field when you select a Media Server as a source.</p> |
| <b>COR</b>       | The Class of Restriction associated with this announcement.                                                                                                                                                                                                                                                                                                               |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tenant Number</b>      | The tenant partition number of the announcement. Valid entries include 1 to 100.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Queue</b>              | <p>The announcement queue or barge-in. The options are:</p> <ul style="list-style-type: none"> <li>• <b>no</b>: Indicates that the announcement is not played if a port is unavailable. This is the default value.</li> <li>• <b>yes</b>: Indicates that the request is placed in a queue when all ports on the circuit pack are busy. The announcement is played when a port becomes available. Most call center applications use this setting.</li> <li>• <b>bargein</b>: Indicates that you can connect callers to the announcement at any time while the announcement is being played. With n or y, the caller is always connected to the beginning of the announcement.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Live Stream Source</b> | <p>The option to stream music on hold live from an external source.</p> <p><b>Live Stream Source</b> is available only when the <b>Type</b> is <b>Integ-mus</b> or <b>Integ-rep</b>.</p> <p>You can select <b>Live Stream Source</b> only when:</p> <ul style="list-style-type: none"> <li>• Queue is set to <b>bargein</b>.</li> <li>• <b>Source</b> is set to Media Server.</li> </ul> <p>If you select <b>Live Stream Source</b>, the system changes the <b>Protected</b> field to Y, which is noneditable.</p> <p>When you deactivate the Release 8.1.3 patch, the system runs on Release 8.1.3 system and sets the <b>Live Stream Source</b> feature to n. Therefore, you must install and activate the new Release 8.1.3 patch immediately to prevent the system processes from running on the Release 8.1.3 system. You must also set the value of the <b>Live Stream Source</b> feature to y.</p> <p> <b>Note:</b></p> <p>After you configure the announcement with Live Stream Source type, play once to ensure that the live streaming feature works correctly.</p> |
| <b>Size</b>               | The size of the audio file in kilobytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Timestamp</b>          | The date and time the audio file was created or modified. This value changes each time you upload the audio file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Audio File Information

| Name                        | Description                                                         |
|-----------------------------|---------------------------------------------------------------------|
| <b>Use Unused Wave File</b> | To use an audio file that has not been used yet.                    |
| <b>Upload Audio File</b>    | To upload an audio file by browsing to the file you want to upload. |

## More Actions

| Name                               | Description                                                                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Broadcast</b>                   | Displays the Broadcast Announcements page.<br><br>You can broadcast the announcements from the Announcement list.<br><br>After the broadcast operation is completed, files are deleted from the SCP server. |
| <b>File Transfer Settings</b>      | Displays the Audio File Transfer Settings page.                                                                                                                                                             |
| <b>Compact Flash Configuration</b> | Displays the Compact Flash Configuration page.                                                                                                                                                              |

## More Actions in Audio Groups

| Name                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b>                                                        | Specifies the filename of the audio file. The filename can be up to 27 characters and must be alphanumeric.                                                                                                                                                                                                                                                                                                                                                                     |
| <b>File Size</b>                                                        | Specifies the size of the audio file in kilobytes.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Backup Announcement Properties</b>                                   | Backs up the announcement property.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Backup Wave Files</b>                                                | Backs up the WAVE files only.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Backup Both (Announcement Properties with associated wave file)</b>  | Backs up both the announcement property and the WAVE file for the announcement.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Restore Announcement Properties</b>                                  | Restores only your announcement properties.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Restore Wave Files</b>                                               | Restores only the wave files present for the announcement.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Restore Both (Announcement Properties with associated wave file)</b> | Restores both the announcement property and the wave file for the announcement.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Source</b>                                                           | This field indicates the source location from where the announcement plays back. <ul style="list-style-type: none"> <li>• The the location of the TN2501 board in the format of cabinet(1-64), carrier(A-E) and slot(1-20). For Example, 03A10</li> <li>• The location of the Media Gateway vVAL in the format of gggV9, where ggg is the gateway number of the media gateway (up to 250).</li> <li>• The Group number (G1-G50) or the Media Server number (M1-M250)</li> </ul> |
| <b>Type</b>                                                             | The whether the Announcement is a VAL Announcement or a Media Gateway (MG) Announcement.                                                                                                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Transfer Mode</b>         | Type of transfer used to backup or restore or upload audio files. Possible values are FTP, SFTP, and, SCP.<br><br>* <b>Note:</b><br>SCP file transfer on gateways, works only with SNMPv3 – MD5 and DES combination. |
| <b>Local SCP Server</b>      | System Manager acts as a SCP server.                                                                                                                                                                                 |
| <b>SCP Server IP Address</b> | When you select <b>Local SCP Server</b> , the system auto populates the <b>SCP Server IP Address</b> field with IP Address of System Manager.                                                                        |
| <b>SCP User Name</b>         | The SCP server user name.<br>If you use <b>Local SCP Server</b> , type the System Manager CLI user name.                                                                                                             |
| <b>SCP Password</b>          | The SCP server password.<br>If you use <b>Local SCP Server</b> , type the System Manager CLI password.                                                                                                               |
| <b>Confirm SCP Password</b>  | Confirm the SCP server password.<br>If you use <b>Local SCP Server</b> , re-type the System Manager CLI password.                                                                                                    |
| <b>Used By</b>               | The object in which the extension is used. For example Endpoint, Announcement etc.                                                                                                                                   |
| <b>Object info</b>           | The details of the object.                                                                                                                                                                                           |
| <b>Used as</b>               | The manner in which the extension is used in the object.                                                                                                                                                             |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Completes the action you initiate.                                  |
| <b>Schedule</b> | Performs the action at the chosen time.                             |
| <b>Reset</b>    | Clears the action and resets the field.                             |
| <b>Clear</b>    | Clears all the entries.                                             |
| <b>Edit</b>     | Edits the fields in the page.                                       |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Download</b> | Downloads the audio files or announcement files.                    |
| <b>Now</b>      | Performs the action you initiate in real time.                      |
| <b>Restore</b>  | Restores your announcements on the voice system you select.         |

## Audio Groups

### What is an audio group?

An audio group is a logical container that holds VAL sources. An audio group can hold several VAL Sources which can be VAL Boards or media gateways.

## Adding an audio group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Audio Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Audio Groups** page and click **Commit**.

### Related links

[Audio Groups field descriptions](#) on page 684

## Editing an audio group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Audio Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the audio group you want to edit.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields and click **Commit** to save the changes.

### Related links

[Audio Groups field descriptions](#) on page 684

## Viewing an audio group

### Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Call Center > Audio Group** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. Select the audio group you want to view.
6. Click **View** to view the properties of the audio group.

### Related links

[Audio Groups field descriptions](#) on page 684

## Deleting an audio group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Audio Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the audio groups you want to delete from the Audio Groups List.
6. Click **Delete**.
7. Confirm to delete the audio groups.

## Using More Actions

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Audio Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select an audio group from the Audio Groups List.
6. Click **More Actions**.
7. Do one of the following:
  - Click **Backup** to back up the audio groups you selected on a voice system.
  - Click **Download** to download the audio groups you selected.
  - Click **Restore** to restore the audio groups on a voice system you select.

### Related links

[Audio Groups field descriptions](#) on page 684

## Audio Groups field descriptions

| Name                | Description                                                          |
|---------------------|----------------------------------------------------------------------|
| <b>System</b>       | The device type. In this case, the Communication Manager you choose. |
| <b>Group Number</b> | The audio group number.                                              |
| <b>Group Name</b>   | The name of the audio group.                                         |

## Members List

| Name             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>    | <p>Specifies whether the VAL board, Media Gateway or Media Server shown is a member in the audio group. Type the group number in the format gggV9 for media gateway vVAL, where <i>ggg</i> is the gateway number of the media gateway (up to 250).</p> <ul style="list-style-type: none"> <li>• The location of the TN2501 board in the format of cabinet(1-64), carrier(A-E) and slot(1-20). For Example, 03A10</li> <li>• The location of the Media Gateway vVAL in the format of gggV9, where <i>ggg</i> is the gateway number of the media gateway (up to 250).</li> <li>• The Media Server number (M1-M250)</li> </ul> |
| <b>Is Member</b> | Specifies whether the VAL board, the Media Gateway or the Media Server shown is a member in the audio group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### **Note:**

You can filter the Members list according to one or multiple columns using the **Filter: Enable** option in the list.

## More Actions in Announcements- field descriptions

| Name                                                                    | Description                                                                     |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>CM</b>                                                               | The Communication Manager you have chosen.                                      |
| <b>Backup Announcement Properties</b>                                   | Backs up the announcement property.                                             |
| <b>Backup Wave Files</b>                                                | Backs up the waves files only.                                                  |
| <b>Backup Both (Announcement Properties with associated wave file)</b>  | Backs up both the announcement property and the wave file for the announcement. |
| <b>File Name</b>                                                        | Name of the audio group.                                                        |
| <b>File Size</b>                                                        | The size of the audio file in kilobytes.                                        |
| <b>Restore Announcement Properties</b>                                  | Restores only your announcement properties.                                     |
| <b>Restore Wave Files</b>                                               | Restores only the wave files present for the announcement.                      |
| <b>Restore Both (Announcement properties with Associated wave file)</b> | Restores both the announcement property and the wave file for the announcement. |
| <b>Restore from client</b>                                              | Select this checkbox if you want to restore from the client machine.            |

| Button          | Description                                |
|-----------------|--------------------------------------------|
| <b>Commit</b>   | Performs the action you initiate.          |
| <b>Schedule</b> | Performs the action at the specified time. |

*Table continues...*

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Reset</b>    | Clears the action and resets the fields.                            |
| <b>Clear</b>    | Clears all the entries.                                             |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Restore</b>  | Restores your announcements on the voice system you select.         |
| <b>Backup</b>   | Backs up the audio files that you select.                           |
| <b>Download</b> | Downloads the audio files or announcement files.                    |
| <b>Now</b>      | Performs the action you initiate real time.                         |

## Holiday Table

### Holiday Table List

Holiday Table List displays all the Holiday Table details under the selected Communication Manager. You can view the usage list of the extension you select in this list. You can also apply filters and sort each of the columns in the Holiday Table List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name          | Description                                                              |
|---------------|--------------------------------------------------------------------------|
| <b>Number</b> | The extension number of the holiday table Number.                        |
| <b>Name</b>   | The name associated with the holiday table.                              |
| <b>System</b> | The name of the Communication Manager associated with the holiday table. |

### Exporting all Holiday Table Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions > Export All Holiday Table**.  
The system displays the **Export Holiday Table** page.
5. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
6. Click **Export**.



## Exporting selected holiday table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. From the **Holiday Table List**, select the holiday table number you want to export.
5. Click **More Actions > Export Selected Holiday Table**.

The system displays the **Export Holiday Table** page.

6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

## Importing holiday table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions > Import Holiday Table**.

The system displays the **Import CM Objects** page.

5. In the **Select a file** field, select the required excel file and click **Browse**.
6. Select one of the following in the **Select Error Configuration** field.

Default value is **Continue processing other records**.

- **Abort on first error**
- **Continue processing other records**

7. Select one of the following in the **If a matching record already exists** field.

Default value is **Skip**.

- **Skip**
- **Merge**
- **Delete**

8. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
9. Click **Import**.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Holiday Table**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions > Download Excel Template**.
5. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

---

## Vector Directory Number

### Vector Directory Number

The Vector Directory Number capability defines the vector directory numbers (VDN) for the Call Vectoring feature. A VDN is an extension number used to access a call vector. Each VDN is mapped to one call vector. VDNs are software extension numbers that is, not assigned to physical equipment. A VDN is accessed through direct dial local telephone company central office trunks mapped to the VDN (incoming destination or night service extension), DID trunks, and LDN calls. The VDN can be Night Destination for LDN.

### Vector Directory Number List

Vector Directory Number List displays all the Vector Directory Number (VDN) details under the selected Communication Manager. You can view the usage list of the extension you select in this list. You can also apply filters and sort each of the columns in the Vector Directory Number List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                      | Description                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Extension</b>          | The extension number of the Vector Directory Number.                                                   |
| <b>Name</b>               | The name associated with the Vector Directory Number.                                                  |
| <b>Destination</b>        | Indicates whether the calls are routed using a Vector Number or Policy Routing Table.                  |
| <b>Destination Number</b> | Indicates the number for <b>Destination</b> .                                                          |
| <b>Allow VDN Override</b> | Indicates whether the routed-to Vector Directory Number is changed to active VDN for the call.         |
| <b>COR</b>                | The Class Of Restriction (COR) of the Vector Directory Number consisting of a one or two-digit number. |
| <b>TN</b>                 | The tenant partition number.                                                                           |

*Table continues...*

| Name          | Description                                                                        |
|---------------|------------------------------------------------------------------------------------|
| <b>System</b> | The name of the Communication Manager associated with the vector directory number. |

## Adding Vector Directory Number

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Vector Directory Number (VDN)** page and click **Commit**.

## Viewing Vector Directory Number

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to view.
6. Click **View**.

## Editing Vector Directory Number

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to edit.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit Directory Number (VDN)** page.
8. Click **Commit** to save the changes.

## Deleting Vector Directory Number

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select the vector directory number you want to delete.
6. Click **Delete**.
7. Confirm to delete the vector directory number.

## List Usage Extension in Vector Directory Number

### Procedure

1. On the System Manager console, under **Elements**, click **Communication Manager**.
2. Click **Call Center > Vector Directory Number** in the left navigation pane.
3. Select a Communication Manager from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Directory Number List, select a vector directory number.
6. Click **More Actions > List Usage Extension**.
7. Click **Done**.

You can view the details of the vector directory number in the List Usage for Extension list.

## Exporting Selected Vector Directory Number

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the **Vector Directory Number List**, select the vector directory number you want to export.
6. Click **More Actions > Export Selected VDN**.

The system displays the **Export VDN** page.

7. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

8. Click **Export**.

## Exporting all Vector Directory Numbers

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Export All VDN**.

The system displays the **Export VDN** page.

6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

## Importing Vector Directory Numbers

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Import VDN's**.

The system displays the **Import CM Objects** page.

6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.

Default value is **Continue processing other records**.

- **Abort on first error**
- **Continue processing other records**

8. Select one of the following in the **If a matching record already exists** field.

Default value is **Skip**.

- **Skip**
- **Merge**
- **Delete**

9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

10. Click **Import**.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Directory Number**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

---

## Vector Routing Table

### Vector Routing Table

Use Vector Routing Table to store ANI or digits that you refer to in the **goto** vector steps. This capability is available only if the **Vectoring (G3V4 Enhanced)** field on the System-Parameters Customer-Options screen is set to **y**.

### Vector Routing Table List

Vector Routing Table List displays all the Vector Routing Tables under the Communication Manager you select. You can also apply filters and sort each of the columns in the Vector Routing Table List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                     | Description                                                                     |
|--------------------------|---------------------------------------------------------------------------------|
| <b>Number</b>            | The table number you entered on the command line.                               |
| <b>Name</b>              | The 1 to 15-character alphanumeric table name. By default, this field is blank. |
| <b>Sort</b>              | Enables you to sort the digit fields.                                           |
| <b>Number Of Entries</b> | The number of entries in the dialing list.                                      |
| <b>System</b>            | The name of the Communication Manager associated with the Vector Routing Table. |

## Adding Vector Routing Table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.

2. In the navigation pane, click **Call Center > Vector Routing Table**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Vector Routing Table** page and click **Commit**.

#### Related links

[Vector Routing Table field descriptions](#) on page 694

## Viewing Vector Routing Table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Routing Table**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing table you want to view.
6. Click **View**.

#### Related links

[Vector Routing Table field descriptions](#) on page 694

## Editing Vector Routing Table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Routing Table**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing table you want to edit.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields on the **Edit Vector Routing Table** page.
8. Click **Commit** to save the changes.

#### Related links

[Vector Routing Table field descriptions](#) on page 694

## Deleting Vector Routing Table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Call Center > Vector Routing Table**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Vector Routing Table List, select the vector routing tables you want to delete.
6. Click **Delete**.
7. Confirm to delete the selected vector routing tables.

### Related links

[Vector Routing Table field descriptions](#) on page 694

## Vector Routing Table field descriptions

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>         | The 1 to 15-character alphanumeric table name or blank. By default, this field is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Number</b>       | The table number you entered on the command line. This is a display-only field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Digit String</b> | <p>Entries in this field can include the plus sign (+) and question mark (?) wildcard. The plus sign (+) represents a group of digits. The question mark (?) represents a single digit. By default, this field is blank.</p> <p>The field is limited to 16 characters and these characters are restricted as follows:</p> <ul style="list-style-type: none"> <li>• You can enter only a plus sign (+), a question mark (?), or the numbers 0 through 9. No other entries are valid.</li> <li>• You can enter a plus sign (+) as either the first or last character in the number field. However, you cannot use this character as the sixteenth character of the number field.</li> <li>• You can use unlimited question marks (?) anywhere in the number field.</li> <li>• You should not embed blanks in the number field.</li> <li>• You can leave the field entirely blank. If you do, the communication server will store the entry as a null value.</li> </ul> |

*Table continues...*



| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sort</b>  | Provides the option to sort the digit fields. By default, this check box is clear. If you do not to sort the numbers, they will remain in the order that you entered them. If you sort the number fields, they will be sorted as described below. Remember that leading zeros are significant. That means that 02 will sort ahead of a 2 followed by a space. <ul style="list-style-type: none"> <li>• Any plus signs (+) will sort first.</li> <li>• Any question marks (?) will sort second.</li> <li>• All numbers (0-9) will sort last.</li> </ul> |
| Route Number | The static route numbers that are available in the selected vector routing table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Completes the action you initiate.                                  |
| <b>Schedule</b> | Performs the action at the chosen time.                             |
| <b>Reset</b>    | Clears the action and resets the field.                             |
| <b>Clear</b>    | Clears all entries.                                                 |
| <b>Edit</b>     | Allows you to edit the fields in the page.                          |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>      | Performs the action you initiate in real time.                      |

## Service Hours Tables

### Service Hours Table List

Service Hours Table displays all the Service Hours Table details under the selected Communication Manager. You can view the usage list of the extension you select in this list. You can also apply filters and sort each of the columns in the Service Hours Table.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name               | Description                                                                    |
|--------------------|--------------------------------------------------------------------------------|
| <b>Number</b>      | The extension number of the service hours table Number.                        |
| <b>Location</b>    | The location associated with the service hours table.                          |
| <b>Description</b> | The description associated with the service hours table .                      |
| <b>System</b>      | The name of the Communication Manager associated with the service hours table. |

## Exporting all Service Hours Table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions > Export All Service Hours**.  
The system displays the **Export Service Hours Table** page.
5. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
6. Click **Export**.

## Exporting selected service hours table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. From the **Service Hours Table List**, select the service hours table number you want to export.
5. Click **More Actions > Export Selected Service Hours**.  
The system displays the **Export Service Hours Table** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

## Importing service hours table

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions > Import Service Hours**.  
The system displays the **Import CM Objects** page.
5. In the **Select a file** field, select the required excel file and click **Browse**.

6. Select one of the following in the **Select Error Configuration** field.

Default value is **Continue processing other records**.

- **Abort on first error**
- **Continue processing other records**

7. Select one of the following in the **If a matching record already exists** field.

Default value is **Skip**.

- **Skip**
- **Merge**
- **Delete**

8. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.

9. Click **Import**.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager > Call Center > Service Hours Tables**.
2. Select one or more Communication Manager instance from the Communication Manager list.
3. Click **Show List**.
4. Click **More Actions > Download Excel Template**.
5. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

---

## Coverage Path

### Coverage Path

Use Coverage Path to implement call coverage paths by providing the means to specify the call coverage criteria, the points in the coverage path used to redirect calls, and the number of times a principal telephone rings before the call redirects to coverage.

### Coverage Path List

Coverage Path List displays all the coverage path details under the Communication Manager you select. You can also apply filters and sort each column in the Coverage Path List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                        | Description                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Coverage Path Number</b> | The coverage path that is being administered.                                                                       |
| <b>Next Path Number</b>     | The number of the next coverage path in a coverage path chain.                                                      |
| <b>Hunt after Coverage</b>  | Indicates whether the coverage treatment is continued or terminated.                                                |
| <b>Number of Rings</b>      | The number of times a telephone rings before the system redirects the call to the first point in the coverage path. |
| <b>System</b>               | The name of the Communication Manager associated with the coverage path.                                            |

## Adding Coverage Path

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Coverage Path** page and click **Commit**.

### Related links

[Coverage Path](#) on page 701

## Viewing a Coverage Path

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to view.
6. Click **View**.

### Related links

[Coverage Path](#) on page 701

## Editing a Coverage Path

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.

3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to edit.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit Coverage Path** page.
8. Click **Commit** to save the changes.

#### Related links

[Coverage Path](#) on page 701

## Deleting a Coverage Path

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Path List, select the coverage path you want to delete.
6. Click **Delete**.
7. Confirm to delete the coverage path.

#### Related links

[Coverage Path](#) on page 701

## Exporting selected Coverage Path

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In **Coverage Path List**, select the coverage path that you want to export.
6. Click **More Actions > Export Selected Coverage Paths**.

The system displays the **Export Coverage Paths** page.

7. In the **Schedule Job** field, click one of the following:
  - **Run immediately**

- **Schedule later**

8. Click **Export**.

## Exporting all Coverage Paths

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Export All Coverage Paths**.  
The system displays the **Export All Coverage Paths** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

## Importing Coverage Paths

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Import Coverage Paths**.  
The system displays the **Import CM Objects** page.
6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.

Default value is **Continue processing other records**.

- **Abort on first error**
- **Continue processing other records**

8. Select one of the following in the **If a matching record already exists** field.

Default value is **Skip**.

- **Skip**
- **Merge**
- **Delete**

9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
10. Click **Import**.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Path**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

## Coverage Path

Implements Call Coverage Paths by providing the means to specify the call coverage criteria, the points in the coverage path used to redirect calls, and the number of times a principal's telephone rings before the call redirects to coverage.

change coverage path 1
Page 1 of 1

**COVERAGE PATH**

Coverage Path Number: 1

Cvg Enabled for VDN Route-To Party? n      Hunt after Coverage? n

Next Path Number:           Linkage

**COVERAGE CRITERIA**

| Station/Group Status | Inside Call | Outside Call |                           |
|----------------------|-------------|--------------|---------------------------|
| Active?              | <u>n</u>    | <u>n</u>     |                           |
| Busy?                | <u>y</u>    | <u>y</u>     |                           |
| Don't Answer?        | <u>y</u>    | <u>y</u>     | Number of Rings: <u>2</u> |
| All?                 | <u>n</u>    | <u>n</u>     |                           |
| DND/SAC/Goto Cover?  | <u>y</u>    | <u>y</u>     |                           |
| Holiday Coverage?    | <u>n</u>    | <u>n</u>     |                           |

**COVERAGE POINTS**

Terminate to Coverage Pts. with Bridged Appearances? y

Point1: 360-5003      Rng:           Point2:                     

Point3:                           Point4:                     

Point5:                           Point6:

## Coverage Path Number

The coverage path being administered.

## Cvg Enabled for VDN Route-To Party

Enables or disables the route-to party coverage path after a covered call hits a VDN vector route-to step. By default, the value is n.

## Holiday Coverage

Use the **Holiday Coverage** field to redirect all calls during a holiday to a coverage path. For **Holiday Coverage** to function, set the **Don't Answer** field to y.

You must set the **Holiday Coverage** field separately for internal and external calls.

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | Communication Manager checks the Holiday Table screen for a specific holiday entry. If an entry on the Holiday Table screen matches with the current date and time, Communication Manager forwards the call to the first point that is defined in the coverage path. If there is no entry that matches with the current date and time, Communication Manager forwards the call to the subsequent point that is defined in the coverage path. |
| n           | Communication Manager forwards the call to the subsequent point in the coverage path.                                                                                                                                                                                                                                                                                                                                                        |

## Holiday Table

Available only when **Holiday Coverage** is set to y for inside or outside calls.

The number of the holiday table used for holiday coverage.

## Hunt After Coverage

| Valid Entry | Usage                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | Coverage treatment continues by searching for an available station in a hunt chain that begins with the hunt-to-station assigned to the station of the last coverage point. |
| n           | Coverage treatment is terminated. The call is left at the last available location, the principal or coverage point.                                                         |

## Linkage

One or two additional coverage paths in the coverage path chain.

## Next Path Number

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 to 9999   | The number of the next coverage path in a coverage path chain. If the coverage criteria of the current coverage path is dissatisfied, the system checks in this chain until it finds a coverage path with redirection criteria that matches the call status. If the chain is exhausted before the system finds a match, the call stays out of coverage. |
| blank       | The only path for the principal.                                                                                                                                                                                                                                                                                                                        |



## Criteria

### Active

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

| Valid Entry | Usage                                                                  |
|-------------|------------------------------------------------------------------------|
| y           | The system redirects the call if at least one call appearance is busy. |
| n           | The system does not redirect the call.                                 |

### Busy

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

| Valid Entry | Usage                                                                                      |
|-------------|--------------------------------------------------------------------------------------------|
| y           | The system redirects the call if all call appearances that accept incoming calls are busy. |
| n           | The system does not redirect the call.                                                     |

### Don't Answer

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

| Valid Entry | Usage                                                                                |
|-------------|--------------------------------------------------------------------------------------|
| y           | The system redirects the call when the specified number of rings have been exceeded. |
| n           | The system does not redirect the call.                                               |

### All

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

| Valid Entry | Usage                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | The system redirects all calls to coverage. This option overrides any other criteria. Calls redirect immediately to coverage. Overrides any other criteria administered for this field. |
| n           | The system does not redirect the call.                                                                                                                                                  |

### DND/SAC/Go to Cover

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

| Valid entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | <p>With this option, a calling user, when calling to another internal extension, can redirect a call immediately to coverage by pressing the <b>Go to Cover</b> button. A principal user can temporarily direct all incoming calls to coverage, regardless of the other assigned coverage criteria by pressing the <b>Send All Calls</b> or <b>Do Not Disturb</b> button. With the <b>Send All Calls</b> button, covering users can temporarily remove their telephones from the coverage path.</p> <p> <b>Note:</b></p> <p>You must assign this criteria before a user can activate <b>Do Not Disturb (Hospitality Services)</b>, <b>Send All Calls (SAC)</b>, or <b>Go to Cover</b> features.</p> |
| n           | The system does not redirect the call.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### **Logged off/PSA/TTI**

Use this field to assign a coverage criteria. When the coverage criteria is met, the system redirects the call to coverage.

The system displays this field only when you set the **Criteria for Logged Off/PSA/TTI Stations** field to y.

| Valid Entry | Usage                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | The system redirects the call after the number of rings exceeds the value specified in the <b>Number of Rings</b> field. The system displays the associated <b>Number of Rings</b> field only when the <b>Logged off/PSA/TTI</b> field is set to y. |
| n           | The system does not redirect the call.                                                                                                                                                                                                              |

### **Number of Rings**

| Valid Entry | Usage                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 to 99     | The number of times a telephone rings before the system redirects the call to the first point in the coverage path. By default, the value is 2. |

### **Coverage points**

#### **Point1, Point2, Point3, Point4, Point5, Point6**

The alternate destinations that comprise a coverage path. Coverage points must be assigned sequentially without steps beginning with Point 1. Each path can have up to six coverage points.

Subsequent coverage points should be unlisted if calls are redirected to:

- Message Center, a special Uniform Call Distribution hunt group
- Voice messaging
- The attendant

These calls normally queue and never redirect to another coverage point. Calls to hunt group queue if possible. Calls redirect from a hunt group only if all hunt group members are busy and either the queue is full, or is nonexistent.

If the Coverage of Calls Redirected Off-Net feature is not supported, a remote coverage point functions as the last point in the coverage path because the system can no longer control calls once they redirect off-net. However, if the Coverage of Calls Redirected Off-Net feature is enabled, calls redirected off-net can be monitored by the system and brought back for call coverage processing.

| Valid Entry   | Usage                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| extension     | Redirects the call to an internal extension or announcement.<br><br>* <b>Note:</b><br>If you enter a shortened extension of the multilocation dial plan, the system does not perform certain administration and validation tasks. Therefore, the system might not display the resultant warnings or submittal denials. |
| attd          | Redirects the call to the attendant or attendant group. If the system has Centralized Attendant Service (CAS), the call goes to the CAS attendant.                                                                                                                                                                     |
| h1 to h8000   | Redirects the call to the corresponding hunt-group, for example, h32 routes to hunt group 32.                                                                                                                                                                                                                          |
| c1 to c1500   | Redirects the call to the corresponding coverage answer group, for example, c20 routes to call coverage answer group 20.                                                                                                                                                                                               |
| r1 to r10000  | Redirects the call to the corresponding remote coverage point number, for example, r27 routes to remote coverage point 27.                                                                                                                                                                                             |
| v + extension | Redirects the call to the corresponding Vector Directory Number (VDN) extension, for example, v12345 routes to the VDN associated with extension 12345.<br><br>* <b>Note:</b><br>A VDN can be used only as the last administered point in a coverage plan.                                                             |
| y + extension | Redirects the call to an internal extension, announcement, or the corresponding Vector Directory Number (VDN) extension as per the current date and time set in Holiday Table.                                                                                                                                         |

### **Rng**

| Valid Entry      | Usage                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------|
| 1 to 99<br>blank | The number of rings at this coverage point before the system redirects the call to the next point in the coverage path. |

### **Terminate to Coverage Pts. with Bridged Appearances**

| Valid Entry | Usage                                                                          |
|-------------|--------------------------------------------------------------------------------|
| y           | If activated, a call can alert as both a bridged call and a redirected call.   |
| n           | The call skips the coverage point if it has already alerted as a bridged call. |

---

## Coverage Time-of-day

### Coverage Time-of-day

Use Coverage Time-of-day to administer up to five different coverage paths associated with five different time ranges, for each day of the week. Only one coverage path can be in effect at a given time.

### Coverage Time-of-day List

Coverage Time-of-day List displays all the coverage time-of-day details under the Communication Manager you select. You can also apply filters and sort each column in the Coverage Time-of-day List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name          | Description                                                                        |
|---------------|------------------------------------------------------------------------------------|
| <b>Number</b> | The Coverage Time-of-day table number.                                             |
| <b>System</b> | The name of the Communication Manager associated with the vector directory number. |

### Adding Coverage Time-of-day

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Time-of-day**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Add Coverage Time-of-day Data** page and click **Commit**.

#### Related links

[Time of Day Coverage Table](#) on page 708

### Viewing Coverage Time-of-day

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Time-of-day**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to view.
6. Click **View**.

#### Related links

[Time of Day Coverage Table](#) on page 708

## Editing Coverage Time-of-day

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Time-of-day**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to edit.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit Coverage Time-of-day Data** page.
8. Click **Commit** to save the changes.

#### Related links

[Time of Day Coverage Table](#) on page 708

## Deleting Coverage Time-of-day

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Coverage > Coverage Time-of-day**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Coverage Time-of-day List, select the coverage time-of-day you want to delete.
6. Click **Delete**.
7. Confirm to delete the coverage time-of-day.

#### Related links

[Time of Day Coverage Table](#) on page 708

## Time of Day Coverage Table

This screen allows administration of up to five different coverage paths, associated with five different time ranges, for each day of the week. Only one coverage path can be in effect at any one time.

change coverage time-of-day 1
Page 1 of 1

TIME OF DAY COVERAGE TABLE: 1

|     | Act<br>Time | Cvg<br>Path | Act<br>Time | Cvg<br>Path | Act<br>Time | Cvg<br>Path | Act<br>Time | Cvg<br>Path | Act<br>Time | Cvg<br>Path |
|-----|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Sun | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |
| Mon | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |
| Tue | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |
| Wed | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |
| Thu | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |
| Fri | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |
| Sat | 0:00        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         | _: _        | ___         |

### Act Time

| Valid Entry  | Usage                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 00:01– 23:59 | <p>Specifies the activation time of the associated coverage path. Information must be entered in 24-hour time format.</p> <p>If there are time gaps in the table, there will be no coverage path in effect during those periods. The first activation time for a day is set to 00:00 and cannot be changed. Activation times for a day must be in ascending order from left to right.</p> |

### CVG Path

| Valid Entry | Usage                     |
|-------------|---------------------------|
| 1 to 9999   | The coverage path number. |
| blank       |                           |

### Time of Day Coverage Table

Displays the Time of Day Coverage Table number.

## Element Cut-Through

### Element Cut-Through

The Element Cut-Through link allows you to access the Communication Manager cut through the Element Cut-Through page. As an administrator you can have various permissions to access the Communication Manager cut through.

- If you have only Communication Manager level access to Communication Manager1 and not Communication Manager2 nor Communication Manager3, then you will see only Communication Manager1 in the list. The other Communication Managers are not shown in the list at all.
- If you have no access to Element Cut-Through on any Communication Manager, then the Cut-Through navigation item will be grayed out or hidden.
- If you have access Element Cut-Through level permissions to some Communication Managers and not others, then the table displays only those Communication Managers that you have permissions.
- If you do not have Element Cut-Through permissions for a given Communication Manager, then the system displays an error message stating that you do not have permission for this operation.

### Accessing Element Cut-Through

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Element Cut-Through**.
3. On the Element Cut-Through page, click on a Communication Manager.

The system displays the Element Cut-Through page.

### Synchronize CM Data and Configure Options / Element Cut-Through field descriptions

#### Synchronize CM Data/Launch Element Cut Through

| Name                   | Description                                                                 |
|------------------------|-----------------------------------------------------------------------------|
| <b>Element Name</b>    | The name of Communication Manager.                                          |
| <b>FQDN/IP Address</b> | The fully qualified domain name or the IP address of Communication Manager. |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Sync Time</b>        | The time when Communication Manager was last synchronized with the Communication Manager database.<br><br>On the standalone System Manager, the last synchronization time zone is that of the System Manager. On the Geographic Redundancy-enabled System Manager, the last synchronization time zone is that of the local system. |
| <b>Last Translation Time</b> | The time when the last translation of Communication Manager has been saved.<br><br>The last translation time zone is always that of the Communication Manager.                                                                                                                                                                     |
| <b>Sync Type</b>             | The type of synchronization. The options are: <ul style="list-style-type: none"> <li>• Initialization</li> <li>• Incremental</li> </ul>                                                                                                                                                                                            |
| <b>Sync Status</b>           | The status of synchronization. The options are: <ul style="list-style-type: none"> <li>• Completed</li> <li>• In progress</li> <li>• Failed</li> </ul>                                                                                                                                                                             |
| <b>Location</b>              | The daylight saving time displayed to set the area code for each location.                                                                                                                                                                                                                                                         |
| <b>Software Version</b>      | The software version of Communication Manager.                                                                                                                                                                                                                                                                                     |
| <b>CM Notification</b>       | The <b>CM Notification</b> is enabled or not while adding a Communication Manager system in System Manager.                                                                                                                                                                                                                        |

### Synchronize CM Data options

| Name                                                 | Description                                                              |
|------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Initialize data for selected devices</b>          | Initializes the data synchronization for selected device.                |
| <b>Incremental Sync data for selected devices</b>    | Executes the incremental data synchronization for selected device.       |
| <b>Execute 'save trans all' for selected devices</b> | Executes the command for saving all the translation for selected device. |
| <b>Audit</b>                                         | Audits the data for selected device.                                     |

| Button                            | Description                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------|
| <b>Now</b>                        | Executes the selected action immediately.                                                |
| <b>Schedule</b>                   | Displays the Job Scheduler page to schedule the data synchronization at a specific time. |
| <b>Launch Element Cut Through</b> | Displays the Element Cut Through page.                                                   |

*Table continues...*



| Button                   | Description                                         |
|--------------------------|-----------------------------------------------------|
| <b>View Audit Report</b> | Displays the Audit Report page.                     |
| <b>Done</b>              | Saves your action and returns to the previous page. |

## Endpoints

### Endpoint management

In System Manager, you can create and manage endpoints using the **Manage Endpoints** option. You can also manage other endpoint related objects such as, Alias Endpoints, Intra Switch CDR, Off PBX Endpoint Mappings, Site Data, and Xmobile Configuration. Additionally, using the **Manage Endpoints** option you can also view, edit, and delete endpoints and other endpoint related objects. System Manager provides support for the following set types:

| Category         | Set Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP/SIP Set types | 9610SIP/9620SIP/9630SIP/9640SIP/9650SIP<br>9608SIP/9621SIP/9641SIP/9611SIP<br>9610/9620/9630/9640/9650<br>9608/9611/9621/9641<br>1603/1608/1616CC<br>9600SIP<br>4620SIP<br>9608SIPCC/9611SIPCC/9621SIPCC/9641SIPCC<br>4610/4620/4621/4622/4625/4630<br>4602+<br>4612CL<br>H.323<br>J129/J169/J169CC/J179/J179CC<br>B199<br> <b>Note:</b> <ul style="list-style-type: none"> <li>Communication Manager Release 8.0.1 and later internally maps the Avaya Conference Phone B199 conference phones with 9630SIP set types.</li> <li>You can administer Avaya Conference Phone B199 conference phones from the System Manager user interface only.</li> </ul> |

*Table continues...*

| Category                                            | Set Type                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCP Set types                                       | 2402/2410/2420<br>9404/9408<br>6402/6402D/6408/6408+/6408D/6408D+/6416D+/6424D+<br>8403B/8405B/8405B+/8405D/8405D+/8410B/8410D/8411B/8411D/8434D<br>1408<br>1416                                                                                                                                                              |
| Analog Set types                                    | 2500, K2500, CallrID, and virtual                                                                                                                                                                                                                                                                                             |
| CS 1000 set types or Avaya Device Adapter set types | CS1k-IP, CS1k-IPCC, CS1k-ana, CS1k-39xx, CS1k-1col, and CS1k-2col                                                                                                                                                                                                                                                             |
| BRI Set types                                       | WCBRI                                                                                                                                                                                                                                                                                                                         |
| X-Mobile endpoints                                  | XMOBILE. Configured as ISDN DECT, IP DECT, PHS, or EC500 type endpoints.<br><br><div>  <b>Note:</b><br/>Endpoints that are configured as XMOBILE cannot access important enhancements to EC500, such as support for SIP trunk groups. </div> |

 **Note:**

The set types supported varies based on the Communication Manager versions managed.

## Adding an endpoint

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. From **Template**, select the template based on the set type you want to add.  
The system auto populates the **Port** and **Set Type** fields.
7. In **Extensions**, perform one of the following:
  - Type the extension number.
  - Click the **Display Extension Ranges** link to select the extension number from the available extension ranges.
8. To add the endpoint, complete the New Endpoint page, and click **Commit**.

Before adding an endpoint, complete the mandatory fields that are marked with a red asterisk (\*). in the **General options**, **Feature Options**, **Site Data**, **Data Module/Analog**

**Adjunct, Abbreviated Call Dialing, Enhanced Call Fwd, Button Assignment, Profile Settings, and Group Membership** sections.

**\* Note:**

To add an endpoint with a non-supported set type, use Element Cut Through. For alias endpoints, choose the corresponding Alias set type from the **Template** field. System Manager automatically creates a template for the Alias set types based on the `aliased-to` set type. Alias endpoint templates have names beginning with `Alias`. Before the system displays the Alias endpoint type template in the drop-down menu, you must create an alias set type on the managed Communication Manager. You can then use the template to add an endpoint.

## Related links

[New Endpoint / Template field descriptions](#) on page 735

## Using Native Name

### Before you begin

To enter the native name:

- You need the Input Method Editor (IME) application.
- You must enable IME.

**\* Note:**

If IME is disabled, the keyboard input remains in the default language.

### About this task

Using the IME application, you can enter characters in multiple languages such as Japanese, Korean, Russian, Arabic, and Chinese without requiring a special keyboard.

The IME icon appears in the Windows system tray and indicates the language that you currently use. For example, if you are using English, the IME icon in the system tray displays **EN**. If you are using French, the IME icon in the system tray displays **FR**.

### Procedure

1. In the Windows system tray, click the IME icon.  
The system displays a list of languages installed on your computer.
2. Select the language that you want to use.
3. On the System Manager web console, click **Users > User Management** and select the native name.

## Editing an endpoint

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.

3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to edit from the Endpoint List.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields in the **Edit Endpoint** page.
8. Click **Commit** to save the changes.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Duplicating an endpoint

### About this task

The Duplicate Endpoint functionality is to support the “duplicate station” command on Communication Manager. Use this functionality to copy information from an existing endpoint and modify it for each new endpoint. For example, you can configure one endpoint as desired for an entire work group. Then, you merely duplicate this endpoint to all the other extensions in the group. Note that only endpoints of the same type can be duplicated. This functionality copies all the feature settings from the selected endpoint to the new endpoints. You can duplicate up to 16 endpoints at one time.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to duplicate from the Endpoint List and click **Duplicate**.
6. On the Duplicate Endpoint page, complete the required fields.
7. Click **Commit** to duplicate the endpoint or do one of the following:
  - Click **Schedule** to duplicate the endpoint at a specified time.
  - Click **Cancel** to cancel the operation.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Viewing an endpoint

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.

3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to view from the Endpoint List.
6. Click **View** to view the attributes of the endpoint you have chosen.

 **Note:**

You cannot edit the fields in the View Endpoint page. To go to the Edit Endpoint page, click **Edit**.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Deleting an endpoint

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint you want to delete from the Endpoint List.
6. Click **Delete**.

The system displays a confirmation message alerting you to a user associated with the endpoint. The system highlights these user-associated endpoints in yellow color.

 **Note:**

You cannot delete an endpoint associated with a user through endpoint management. You can delete the user associated endpoints only through User Profile Management.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Saving an endpoint as a template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.

6. Select the template based on the set type you want to add, and complete the New Endpoint page.
7. To save the current settings as a template, click **Save As Template**.
8. Enter the name of the template in the **Template Name** field.
9. Click **Save**.
10. Click **Commit**.

## Editing endpoint extensions

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the endpoint from the Endpoint List for which you want to edit the extension.
6. Click **More Actions > Edit Endpoint Extension**.
7. Complete the **Edit Endpoint Extension** page and click **Commit** to save the new extension.

#### **Note:**

You can use the **Edit Endpoint Extension** option to change the endpoint extension. You can also edit the **Message Lamp Ext** and **Emergency Location Ext** fields through **Edit Endpoint Extension**. Use the **Edit** option to modify the other attributes.

### Related links

[Edit Endpoint Extension field descriptions](#) on page 769

## Bulk adding endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Bulk Add Endpoints**.
6. Complete the **Bulk Add Endpoint** page and click **Commit** to bulk add the endpoints.

The **Endpoint Name Prefix** field gives the common prefix which appears for all the endpoints you bulk add. You can enter any prefix name of your choice in this field.

In the **Enter Extensions** field, enter the extensions that you want to use. You must enter the extensions in a serial order and also check for the availability of an extension before you use it.

 **Note:**

With Multi Tenancy, when you add endpoints in bulk, the Communication Manager devices and the extension range are available according to the Site you selected in the Communication Manager List page. **Tenant Number** and **Location** fields are auto populated for all the endpoints according to the Site you selected.

**COR** and **COS** fields are validated as per the tenant permissions when you add the endpoints in bulk.

### Related links

[Bulk Add Endpoint field descriptions](#) on page 769

## Deleting endpoints in bulk

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **More Actions > Bulk Delete Endpoints**.
6. On the Bulk Delete Endpoints page, select the Communication Manager from the **System** field.
7. Do one of the following:
  - Select the extension range you want to delete from the **Existing Extensions** field.
  - Type the extensions you want to bulk delete in the **Enter Extensions** field.
8. Click **Continue**.
9. On the Bulk Delete Endpoint Confirmation page, click **Now**.  
Click **Schedule** to schedule the bulk delete at a later time.

 **Note:**

You cannot delete user associated stations.

## Filtering endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.

3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Endpoint List.
6. Filter the endpoints according to one or multiple columns.
7. Click **Apply**.

To hide the column filters, click **Disable**. This action does not clear any filter criteria that you have set.

 **Note:**

The table displays only those endpoints that match the filter criteria.

### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Using Advanced Search

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Advanced Search** in the Endpoint list.
6. In the Criteria section, do the following:
  - a. Select the search criterion from the first drop-down field.
  - b. Select the operator from the second drop-down field.
  - c. Enter the search value in the third field.

If you want to add a search condition, click the plus sign (+) and repeat the sub steps listed in Step 5.

If you want to delete a search condition, click the minus sign (-). This button is available if there is more than one search condition.

### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Changing endpoint parameters globally

### About this task

Use the Global Endpoint Change capability to edit endpoint properties in bulk across one or more Communication Manager systems.



You can change the endpoint properties manually or change the endpoint properties based on a default template. You can select your preferred default template from the **Template Name** list on the **General Options** tab. When you select your preferred default template, the system overwrites the field values in different property tabs, such as General Options, Feature Options, and Button Assignment, with values in the default template. You can modify the endpoint properties of the default template to meet your requirement. The customization does not impact the default template because the system applies the changes only to the listed extensions.

For example, you can find all buttons or features with a specific assign and change the parameters for all those buttons or features respectively, locate new buttons without overwrite, and change the set type of many endpoints simultaneously as you move from digital to IP or SIP.

## Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, select the endpoints from the list for which you want to change the parameters.
4. Select one or more Communication Manager instance from the Communication Manager list.
5. Click **Show List**.
6. Select one or more endpoints, click **More Actions > Global Endpoint Change**.

The system displays the Endpoint Changes page.

7. Click the General Options tab, and select **Set Type** to update the template.

### **Note:**

If you also change the **Set Type** while updating the station, the default value overwrites the value in the **Port** field. The options for the default values are X and IP. Therefore, you must manually change the **Port** value for each station.

8. On the Endpoint Changes page, set the error configuration option in **Select Error Configuration**. The options are:
  - **Continue processing other records:** When you select this option, the system skips the erroneous record and continues to process the other records. This is the default setting.
  - **Abort on first error:** When you select this option, the system aborts the importing process on encountering the first error.
9. Do one of the following:
  - Modify the fields in each of the tabs as required.
  - In the General Options tab, select your preferred default template from the **Template Name** field, and update the property fields as required.

The system overwrites all the field values with the values in the template. This update does not affect the default template because the system applies the changes only to the listed extensions.

10. Do one of the following:

- To change the endpoint parameters immediately, click **Commit**.
- To change the endpoint parameters at a specified time, click **Schedule**.

The system updates the selected endpoints or schedules the edit job to the specified time.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

## Viewing endpoint status

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. From the Endpoint List, select the endpoints whose status you want to view.
4. Click **Maintenance > Status**.

### Result

The system displays the status of the selected endpoint on the Element Cut Through screen.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

[Error codes](#) on page 770

## Busy out endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select the endpoints you want to busy out from the Endpoint List.

#### Important:

This maintenance operation is service affecting.

4. Click **Maintenance > Busyout Endpoint**.
5. On the Busyout Endpoint Confirmation page, click **Now** to busy out the endpoints or do one of the following:
  - Click **Schedule** to perform the busy out at a specified time.
  - Click **Cancel** to cancel the busy out.

### Result

The system displays the result of the busy out operation on the **Busyout Endpoint Report** page.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

[Error codes](#) on page 770

## Releasing endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select the endpoints you want to release from the Endpoint List.

#### **Important:**

This maintenance operation is service affecting.

4. Click **Maintenance > Release Endpoint**.
5. On the **Release Endpoint Confirmation** page, click **Now** to release the endpoints or do one of the following:
  - Click **Schedule** to perform the release at a specified time.
  - Click **Cancel** to cancel the release.

### Result

The system displays the result of the release operation on the **Release Endpoint Report** page.

### Related links

[New Endpoint / Template field descriptions](#) on page 735

[Error codes](#) on page 770

## Testing endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select the endpoints you want to test from the Endpoint List.

#### **Important:**

This maintenance operation is service affecting.

4. Click **Maintenance > Test Endpoint**.
5. On the Test Endpoint Confirmation page, click **Now** to test the endpoints or do one of the following:
  - Click **Schedule** to test the endpoints at a specified time.
  - Click **Cancel** to cancel the test operation.

### Result

The system displays the **Test Endpoint Report** page, where you can view the test result and error code of the endpoint. Click the **Error Code Description** link to view the error details.

## Related links

[New Endpoint / Template field descriptions](#) on page 735

[Error codes](#) on page 770

## Using Clear AMW All

**Clear AMW All** is one of maintenance operations listed under the **Maintenance** drop-down on the Manage Endpoints page. You can perform this operation on a single or multiple endpoints from the Endpoint List. In this maintenance operation, for each endpoint, the system runs the following SAT command

```
clear amw all <endpoint>
```

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select the endpoints from the Endpoint List for which you want to use this functionality.
4. Click **Maintenance > Clear AMW All**.
5. On the **Clear AMW All Confirmation** page, click **Now** to perform this task immediately, or do one of the following:
  - Click **Schedule** to perform this task at a specified time.
  - Click **Cancel** to cancel this task.

The system displays a confirmation that the command has been completed and returns you to the Manage Endpoint landing page.

## Using Swap Endpoints

### About this task

Use this functionality to swap location site data between two endpoints of the same type and the same Communication Manager system. For Analog and DCP endpoint types, this functionality also swaps the physical port information. While swapping the endpoint data, you also have the option to assign new location site data to the endpoints.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Swap Endpoints**.
6. On the Swap Endpoints page, enter endpoint extension values in the fields **Endpoint 1** and **Endpoint 2**.

7. Click **Show Details**. The system displays the location site data for each endpoint under the respective endpoint tabs.
8. Click **Commit** to swap data between the two endpoints.
9. To assign new values to the endpoints, perform the following:
  - a. Click the endpoint tab whose data you want to change.
  - b. Select the **Assign data for Endpoint<n>** check box.
  - c. Enter the required values for the endpoint under **Descriptions**.
  - d. Click **Commit**.

### Related links

[Swap Endpoints field descriptions](#) on page 770

[New Endpoint / Template field descriptions](#) on page 735

## Endpoint list

The endpoint list displays all endpoints associated with Communication Manager that you select. You can perform an advanced search on the endpoint list by using the search criteria. You can apply filters and sort each of the columns in the endpoint list.

| Name                 | Description                                            |
|----------------------|--------------------------------------------------------|
| <b>Name</b>          | The endpoint name.                                     |
| <b>Extension</b>     | The extension of the endpoint.                         |
| <b>Port</b>          | The port of the endpoint.                              |
| <b>Set Type</b>      | The set type of the endpoint.                          |
| <b>COS</b>           | Class Of Service for the endpoint.                     |
| <b>COR</b>           | Class Of Restriction for the endpoint.                 |
| <b>User</b>          | The user to which the endpoint is associated.          |
| <b>Tenant Number</b> | The tenant number to which the endpoint is associated. |
| <b>System</b>        | Communication Manager of the endpoint.                 |

| Button         | Description                                                                        |
|----------------|------------------------------------------------------------------------------------|
| <b>Refresh</b> | Displays the updated information that is available after the last synchronization. |

## Exporting selected endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. In **Endpoint List**, select the endpoint that you want to export.
6. Click **More Actions > Export Selected Endpoints**.  
The system displays the **Export Endpoints** page.
7. In the **Schedule Job** field, click one of the following:
  - **Run immediately**
  - **Schedule later**
8. Click **Export**.

## Exporting all endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Export All Endpoints**.  
The system displays the **Export All Endpoints** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

## Importing endpoints

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Import Endpoints**.  
The system displays the **Import CM Objects** page.
6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.  
Default value is **Continue processing other records**.
  - **Abort on first error**

- **Continue processing other records**
8. Select one of the following in the **If a matching record already exists** field.  
Default value is **Skip**.
    - **Skip**
    - **Merge**
    - **Delete**
  9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
  10. Click **Import**.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and then click **OK**.

## Migration of J1xx endpoints configured as 96x1 SIP set type

If a J-Series endpoint is configured as 96x1 SIP set type on Communication Manager, then from System Manager Release 8.1.3, you can migrate that to J1xx set type. To migrate the set type:

- System Manager and Session Manager must be on Release 8.1.3 and later.
- Communication Manager must be on Release 8.x and later.
- J1xx phone must be on Release 4.0.6.0 and later. It must be registered at least once to Session Manager Release 8.1.3 and later.

### Criteria for migrating 96x1 SIP set type to J1xx set type

If **Current Set Type** configured on Communication Manager is one of the non-Contact Center set types 9608SIP, 9611SIP, 9621SIP, 9641SIP or Contact Center set types 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, or ALIAS of any of these set types, and if a user has one of the following, System Manager marks an endpoint eligible.

- One device connected of type J129, J139, J159, J169, J179, or J189.
- More than one devices connected and has at least one device of type J129, J139, J159, J169, J179, or J189.

When an endpoint is eligible for migration, you can migrate the endpoint to specific Set type(s).

1. If **Current Set Type** configured on Communication Manager is one of the non-Contact Center set types 9608SIP, 9611SIP, 9621SIP, or 9641SIP, then you can migrate to the endpoint as described in the following table.

| Set type | Migrate to |
|----------|------------|
| J129     | J129       |
| J139     | J179       |
| J159     | J179       |
| J169     | J169       |
| J179     | J179       |
| J189     | J179       |

For multiple connected devices, System Manager always displays J179 as the preferred set type in the list of allowed set type for migration.

2. If **Current Set Type** configured on Communication Manager is one of the Contact Center set types 9608SIPCC, 9611SIPCC, 9621SIPCC, or 9641SIPCC, then migrate to the endpoint as described in the following table.

| Set type | Migrate to |
|----------|------------|
| J129     | J179CC     |
| J139     | J179CC     |
| J159     | J179CC     |
| J169     | J169CC     |
| J179     | J179CC     |
| J189     | J179CC     |

For multiple connected devices, System Manager always displays J179CC as the preferred set type in the list of allowed set type for migration.

## Discover 96x1 SIP set type ready for J1xx migration

You can discover the endpoints that are ready for J1xx migration by enabling the **Discover Endpoints Eligible for Migration** job on the **Services > Scheduler > Pending Jobs** page.

By default, the **Discover Endpoints Eligible for Migration** job is disabled. You cannot edit and perform **Schedule Job On Demand** settings for this job.

When the **Discover Endpoints Eligible for Migration** job is executed, System Manager:

- Processes all endpoints on all Communication Managers that have a user associated on the **Users > User Management > Manage Users** page.

For information about the J1xx migration criteria, see “Criteria for migrating 96x1 SIP set type to J1xx set type”.



- Marks the endpoint as **Migration Eligible** on the **Elements > Communication Manager > Endpoints > Manage Endpoints** page, if it meets the current and connected set type criteria.

 **Note:**

System Manager automatically disables the discovery job details after 31 days. If required, the administrator can enable the discovery job again.

Once the **Discover Endpoints Eligible for Migration** job is executed at least once, you can perform an advanced search to see the list of endpoints that are ready for migration.

If any new user is added in System Manager that meets migration criteria, then System Manager processes the endpoint in the next execution of discover job.

### Related links

[Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search](#) on page 727

## Enabling the Discover Endpoint eligible for migration job

### Procedure

1. On the System Manager web console, click **Services > Scheduler > Pending Jobs**.
2. In the Job List section, select the **Discover Endpoints Eligible for Migration** job, and click **Enable**.
3. On the Enable Confirmation page, click **Continue**.

After enabling the **Discover Endpoints Eligible for Migration** job, it executes daily at 1 A.M according to the System Manager server timezone and continues for 31 days. Once the job completes for consecutive 31 days, System Manager disables the job automatically.

## Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search

### About this task

On the Manage Endpoint page, System Manager displays the list of endpoints eligible for migration that were discovered in its last run of the **Discover Endpoints Eligible for Migration** job.

 **Note:**

If some endpoints have already been migrated to J-Series phones, System Manager does not display those endpoints.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. In the **Endpoint List** section, click **Advanced Search**.
6. In the Criteria section, do the following:
  - a. From the first drop-down field, select the search criterion **Endpoint General**.
  - b. From the second drop-down field, select the operator **Migration Eligible**.
  - c. From the third drop-down field, select the operator **true**.

The options are:

- **true**
- **false**

By default, the value of **Migration Eligible** is set to **false**.

If you want to add a search condition, click the plus sign (+) and select the new criteria as required.

If you want to delete a search condition, click the minus sign (-). This button is available if there is more than one search condition.

7. Click **Search**.

System Manager displays the endpoints that meet the search criteria in the Endpoint List section.

## Related links

[Discover 96x1 SIP set type ready for J1xx migration](#) on page 726

## Migrating set type of selected J1xx endpoint from 96x1 SIP to J1xx set type

### About this task

If a station is configured on Communication Manager with set types 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, or 9641SIPCC and if there are one or more J-Series phone with type J129, J139, J159, J169, J179, then you must change the set type on Communication Manager or migrate set type to any of the J129, J169, J179, J169CC, J179CC set types.

### **Note:**

- If there are multiple set types, it is recommended to choose a set type that has more feature capabilities. If you select a set type that has lesser feature capabilities, it can result in loss of functionality on that endpoint after the migration.
- For Contact Center set types, select the Contact Center set-type only.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.

5. Search for endpoints ready for migration by using **Advanced Search**.

For information, see “Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search”.

6. Select one or more endpoint, click **More Actions > Migrate Selected Endpoints**.

System Manager displays the Endpoint Migration page.

Depending on the number of connected devices, System Manager displays the 96x1 endpoints that are ready for migration either on the **Same Set-type(s)** tab or on the **Different Set-types** tab.

7. To migrate endpoints that are available on the **Same Set-type(s)** tab, in the Migrate Endpoint List section, do the following:

- a. Select one or more endpoints.
- b. Click **Create New Job**.

8. To migrate endpoints that are available on the **Different Set-types** tab, in the Migrate Endpoint List section, do the following:

a. Do one of the following:

- Select one or more endpoint, and select the set type you want to migrate to in the **Set Type After Migration** column.

Based on **Connected Set Type**, System Manager displays the values in the **Set Type After Migration** column.

For more information, see the “96x1 endpoint to J100-Series migration criteria” section.

- Select one or more endpoint, select the **Default for Set Type After Migration** check box, and then select the default set type you want to migrate to from the drop-down list.

 **Note:**

- If you select the default set type option and also select a value in the **Set Type After Migration** column for one or more endpoints, then System Manager gives precedence to the **Set Type After Migration** column value for migrating the endpoints where the value is provided and migrates all other endpoints to the default set type.
- If the selected default set type is not applicable for one or more endpoints, then migration of those endpoints fail.

b. Click **Create New Job**.

9. On the Migrate Endpoints page, in the Schedule section, perform one of the following:

- Select **Run immediately** to execute the job now.
- Select **Schedule later** to execute the job at a later time.

10. Click **Migrate Endpoints**.

System Manager displays the job status on the:

- **Services > Scheduler > Completed Jobs** page.
- **Endpoint Migration Job History** tab.

**Related links**

[Criteria for migrating 96x1 SIP set type to J1xx set type](#) on page 725

[Enabling the Discover Endpoint eligible for migration job](#) on page 727

[Searching for 96x1 SIP set type for J1xx endpoint migration by using advanced search](#) on page 727

[Endpoint Migration field descriptions](#) on page 733

## Migrating set type of all J1xx endpoint from 96x1 SIP to J1xx set type

### About this task

If a station is configured on Communication Manager with set types 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, or 9641SIPCC and if there are one or more J-Series phone with type J129, J139, J159, J169, J179, then you must change the set type on Communication Manager or migrate set type to any of the J129, J169, J179, J169CC, J179CC set types.

 **Note:**

- If there are multiple set types, it is recommended to choose a set type that has more feature capabilities. If you select a set type that has lesser feature capabilities, it can result in loss of functionality on that endpoint after the migration.
- For Contact Center set types, select the Contact Center set-type only.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Migrate All Endpoints Ready for Migration**.

System Manager displays the Endpoint Migration page.

Depending on the number of connected devices, System Manager displays the 96x1 endpoints that are ready for migration either on the **Same Set-type(s)** tab or on the **Different Set-types** tab.

6. To migrate endpoints that are available on the **Same Set-type(s)** tab, in the Migrate Endpoint List section, do the following:
  - a. Select one or more endpoints.

- b. Click **Create New Job**.
7. To migrate endpoints that are available on the **Different Set-types** tab, in the Migrate Endpoint List section, do the following:
  - a. Do one of the following:
    - Select one or more endpoint, and select the set type you want to migrate to in the **Set Type After Migration** column.

Based on **Connected Set Type**, System Manager displays the values in the **Set Type After Migration** column.

For more information, see the “96x1 endpoint to J100-Series migration criteria” section.

    - Select one or more endpoint, select the **Default for Set Type After Migration** check box, and then select the default set type you want to migrate to from the drop-down list.

 **Note:**

- If you select the default set type option and also select a value in the **Set Type After Migration** column for one or more endpoints, then System Manager gives precedence to the **Set Type After Migration** column value for migrating the endpoints where the value is provided and migrates all other endpoints to the default set type.
  - If the selected default set type is not applicable for one or more endpoints, then migration of those endpoints fail.
- b. Click **Create New Job**.
  8. On the Migrate Endpoints page, in the Schedule section, perform one of the following:
    - Select **Run immediately** to execute the job now.
    - Select **Schedule later** to execute the job at a later time.
  9. Click **Migrate Endpoints**.

System Manager displays the job status on the:

- **Services > Scheduler > Completed Jobs** page.
- **Endpoint Migration Job History** tab.

#### Related links

[Criteria for migrating 96x1 SIP set type to J1xx set type](#) on page 725

[Enabling the Discover Endpoint eligible for migration job](#) on page 727

[Endpoint Migration field descriptions](#) on page 733

### Viewing endpoint migration job history

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.

2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Perform one of the following:
  - Select an eligible endpoint and click **More Actions > Migrate Selected Endpoints**.
  - Click **More Actions > Migrate All Endpoints Ready for Migration**.

System Manager displays the Endpoint Migration page.

6. Click **Endpoint Migration Job History**.
7. Select a job and click **View Job Details**.

System Manager displays the Endpoint Migration Job Details page with the number of successfully migrated endpoints and list of endpoints that have failed during migration. In the Endpoints Failed List section, you can view the failed endpoint and its cause of failure.

## Cancelling an endpoint migration job

### About this task

You can cancel only one job at a time.

### Before you begin

Ensure that the job is in the **RUNNING** state.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Perform one of the following:
  - Select an eligible endpoint and click **More Actions > Migrate Selected Endpoints**.
  - Click **More Actions > Migrate All Endpoints Ready for Migration**.

System Manager displays the Endpoint Migration page.

6. Click **Endpoint Migration Job History**.
7. In the Endpoint Migration Job History section, select a job, and click **Cancel Job**.

System Manager displays the confirmation message.
8. Click **OK**.

System Manager cancels the selected job.

## Deleting endpoint migration job

### About this task

If the job is in the **RUNNING** state, you cannot delete that job.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Perform one of the following:
  - Select an eligible endpoint and click **More Actions > Migrate Selected Endpoints**.
  - Click **More Actions > Migrate All Endpoints Ready for Migration**.

System Manager displays the Endpoint Migration page.

6. Click **Endpoint Migration Job History**.
7. In the Endpoint Migration Job History section, select a job, and click **Delete Job**.

System Manager displays the confirmation message.

8. Click **OK**.

System Manager deletes the selected job.

## Endpoint Migration field descriptions

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Same Set-type(s)</b>               | Displays the list of endpoints that are connected to the same set type. <ul style="list-style-type: none"> <li>• If a user has one device connected, then System Manager displays it under <b>Same Set-type(s)</b>.</li> <li>• If a user has more than one devices connected and all are of the same type, then System Manager categorizes the devices as a same set type and displays under <b>Same Set-type(s)</b>.</li> </ul> |
| <b>Different Set-types</b>            | Displays the list of endpoints that are connected to different set type.<br>If a user has more than one devices connected and has different combinations of set types, then System Manager displays the device under <b>Different Set-types</b> .                                                                                                                                                                                |
| <b>Endpoint Migration Job History</b> | Displays the history of endpoint migration jobs.                                                                                                                                                                                                                                                                                                                                                                                 |

### Migrate Endpoint List

The Migrate Endpoint List section displays all endpoints that are ready for migration. You can apply filters and sort each of the columns.

| Name                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default for Set Type After Migration</b> | <p>The default set type you want to migrate to.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>J129</b></li> <li>• <b>J169</b></li> <li>• <b>J179</b></li> <li>• <b>J169CC</b></li> <li>• <b>J179CC</b></li> </ul> <p> <b>Note:</b></p> <p>If the selected default type is not available in the <b>Set Type After Migration</b> column for an endpoint, then the migration fails.</p>                                           |
| <b>Name</b>                                 | The name of the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Extension</b>                            | The extension of the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Current Set Type</b>                     | The current set type of the endpoint that is configured on Communication Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Connected Set Type</b>                   | The connected set type of the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Set Type After Migration</b>             | <p>The set type after migration of the endpoint.</p> <p>Based on <b>Connected Set Type</b>, System Manager displays the values in the <b>Set Type After Migration</b> column.</p> <p> <b>Note:</b></p> <p>You must select a set type that has more capabilities in the <b>Set Type After Migration</b> column. If you select a set type that has lesser capabilities, it can result in loss of functionality on that endpoint after the migration.</p> |
| <b>User</b>                                 | The user to which the endpoint is associated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Tenant Number</b>                        | The tenant number to which the endpoint is associated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>System</b>                               | The Communication Manager name of the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Button                | Description                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------------------|
| <b>Create New Job</b> | Displays the Migrate Endpoints page to schedule the endpoint migration job immediately or at a later time. |
| <b>Cancel</b>         | Cancels the changes and returns to the Manage Endpoints page.                                              |

### Endpoint Migration Job History field descriptions

| Name              | Description                                      |
|-------------------|--------------------------------------------------|
| <b>Start Time</b> | The date and time the job is scheduled to start. |
| <b>End Time</b>   | The date and time the job execution completes.   |

*Table continues...*



| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Status</b>          | The status of the job can be: <ul style="list-style-type: none"> <li>• <b>SUCCESSFUL</b>: When the endpoint migration job is successfully completed.</li> <li>• <b>FAILED</b>: When the endpoint migration job is failed.</li> <li>• <b>PARTIAL_FAILURE</b>: When the endpoint migration job partially fails.</li> <li>• <b>INTERRUPTED</b>: When the endpoint migration job is canceled.</li> <li>• <b>RUNNING</b>: When the endpoint migration job is in progress.</li> <li>• <b>PENDING_EXECUTION</b>: When the endpoint migration job is scheduled.</li> </ul> |
| <b>Job Name</b>        | The job name as displayed on the Scheduler page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Scheduled By</b>    | The name of user who created the job                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Total Scheduled</b> | The total number of records scheduled for migration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Processed*</b>      | The total number of processed records.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Successful</b>      | The total number of successful records.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Failed</b>          | The total number of failed records.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Not Processed*</b>  | The total number of unprocessed records.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

 **Note:**

\*: These fields are available only on the Endpoint Migration Job Details page.

| Button                  | Description                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Job Details</b> | Displays the Endpoint Migration Job Details page with the number of successfully migrated endpoints and list of endpoints that have failed during migration. |
| <b>Cancel Job</b>       | Cancels one job at a time. The job must be in the <b>RUNNING</b> state.                                                                                      |
| <b>Delete Job</b>       | Deletes one or more job. You cannot delete the job that is in the <b>RUNNING</b> state.                                                                      |

### Endpoint Migration Job Details: Endpoints Failed List

| Name                 | Description                                     |
|----------------------|-------------------------------------------------|
| <b>Extension</b>     | The extension of the failed endpoint.           |
| <b>CM Name</b>       | The Communication Manager name of the endpoint. |
| <b>Error Message</b> | The cause of failure.                           |

## Add Endpoint Template

### New Endpoint / Template field descriptions

Use the fields to perform endpoint or template tasks. The page displays exclusive fields that occur for endpoints and templates apart from the **General options**, **Feature Options**, **Site Data**, **Data**

**Module/Analog Adjunct, Abbreviated Call Dialing, Enhanced Call Fwd, and Button Assignment** sections.

### Field descriptions for Endpoints

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>   | Communication Manager to which the endpoint is assigned.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Template</b> | Template that correspond to the set type of the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Set Type</b> | The set type or the model number of the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Name</b>     | <p>The name of the endpoint. The system displays the name on called telephones with display capabilities. In some messaging applications, such as Communication Manager Messaging, you enter the user name (last name first) and the extension to identify the telephone. The name is also used in the integrated directory.</p> <p>When you enter the first name and the last name of the user associated with an endpoint on User Management, the system populates Latin translation of the first name and the last name in the <b>Name</b> field.</p> |

### Field descriptions for Templates

| Name                 | Description                                                                             |
|----------------------|-----------------------------------------------------------------------------------------|
| <b>Set Type</b>      | The set type or the model of the endpoint template.                                     |
| <b>Template Name</b> | The name of the endpoint template. You can enter the name of your choice in this field. |

| Button          | Description                                                           |
|-----------------|-----------------------------------------------------------------------|
| <b>Commit</b>   | Saves the values that you enter and starts the add or edit operation. |
| <b>Schedule</b> | Displays the Job Scheduler where you can schedule the edit operation. |
| <b>Reset</b>    | Clears the values that you enter on the page.                         |
| <b>Cancel</b>   | Cancels the current operation and returns to the previous page.       |

### Extension

The extension for this station.

For a virtual extension, a valid physical extension or a blank can be entered. With blank, an incoming call to the virtual extension can be redirected to the virtual extension “busy” or “all” coverage path.

The extension length must be within 16 digits.

### Port

The Auxiliary and Analog ports assigned to the station are as follows.

| Valid Entry | Usage                                                 |
|-------------|-------------------------------------------------------|
| 01 to 64    | The first and second numbers are the cabinet numbers. |

*Table continues...*

| Valid Entry       | Usage                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A to E            | The third character is the carrier.                                                                                                                                                                                                                                                                                                                             |
| 01 to 20          | The fourth and fifth characters are the slot numbers. G650 has 14 slots.                                                                                                                                                                                                                                                                                        |
| 01 to 32          | The sixth and seventh characters are the port numbers.                                                                                                                                                                                                                                                                                                          |
| x or X            | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.            |
| IP                | Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers. |
| xxxVmpp           | Specifies the Branch Gateway. <ul style="list-style-type: none"> <li>• xxx is the Branch Gateway number, which is in the range 001 to 250.</li> <li>• m is the module number, which is in the range 1 to 9.</li> <li>• pp is the port number, which is in the range 01 to 32.</li> </ul>                                                                        |
| Analog Trunk port | Analog trunk port is available with: <ul style="list-style-type: none"> <li>• MM711 and MM714 media modules</li> <li>• TN747 and TN797 circuit packs</li> </ul>                                                                                                                                                                                                 |

### General Options

Use this section to set the general fields for a station.

#### COR

Class of Restriction (COR) number with the required restriction.

#### COS

The Class of Service (COS) number used to select allowed features.

#### Emergency Location Ext

The Emergency Location Extension for this station. This extension identifies the street address or nearby location when an emergency call is made. Defaults to the telephone's extension. Accepts up to sixteen digits.

#### Note:

On the ARS Digit Analysis Table in Communication Manager, 911 must be administered to be call type emer or alrt for the E911 Emergency feature to work properly.

#### Message Lamp Ext

The extension of the station tracked with the message waiting lamp.

#### TN

Use this field to specify a tenant number. You can enter a value from 1 to 250.

#### Coverage Path 1 or Coverage Path 2

The coverage-path number or time-of-day table number assigned to the station.

#### \* **Note:**

If Modified Misoperation is active, a Coverage Path must be assigned to all stations on Communication Manager.

#### Lock Messages

Controls access to voice messages by other users.

| Valid Entry | Usage                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| y           | Restricts other users from reading or canceling the voice messages, or retrieving messages using Voice Message Retrieval. |
| n           | Allows other users to read, cancel, or retrieve messages.                                                                 |

#### Multibyte Language

When you configure endpoints, if the localized display name contains multiscrypt language characters, then you must set the locale or multibyte language. You can set the locale using the **Multibyte Language** field. The possible values for the **Multibyte Language** field are:

- Japanese
- Simplified Chinese
- Traditional Chinese
- Not Applicable

In **User Management > Manage Users > Identity**, if you choose the Simplified Chinese, Traditional Chinese, or Japanese from the **Language Preference** field for a user, the appropriate language is auto populated in the **Multibyte Language** field for the same user. If you choose any other language from the **Language Preference** field, the system displays **Not Applicable** in the **Multibyte Language** field.

#### Continue on Error

When an error occurs, the system provides an option to continue or abort the implementation of parameter changes.

#### Security Code

The security code required by users for specific system features and functions are as follows:

- Extended User Administration of Redirected Calls
- Personal Station Access
- Redirection of Calls Coverage Off-Net
- Leave Word Calling

- Extended Call Forwarding
- Station Lock
- Voice Message Retrieval
- Terminal Self-Administration
- Enterprise Mobility User
- Extension to Cellular
- Call Forwarding
- Posted Messages
- Security Violation Notification
- Demand Printing

The required security code length is administered system wide.

#### Primary Session Manager

The IPv4 and IPv6 addresses of the primary Session Manager.

If the call to the SIP station is routed to a SIP trunk that has a clustered signaling group, then the Invite is sent to the station on primary Session Manager.

#### Secondary Session Manager

The IPv4 and IPv6 addresses of the secondary Session Manager.

If the call to the SIP station is routed to a SIP trunk that has a clustered signaling group and the primary Session Manager is not reachable, then the Invite is sent to the station on secondary Session Manager.

#### **Note:**

Primary Session Manager and Secondary Session Manager fields can be configured from the User Management pane only. You cannot configure these fields from the Manage Endpoint page or Element Cut-through page.

#### System ID

This field can be configured for CS 1000 station types only. This field allows you to leave the field blank or enter a string of up to 9 characters. With Release 8.0 and later, more than one station can use the combination of **System ID** and **Terminal Number**.

With Release 8.0.1 and later, each station must have a unique combination of **System ID** and **Terminal Number**.

#### Terminal Number

This field can be configured for CS 1000 station types only. You can enter numbers in the following range: 0.0.0.0 to 252.1.15.31.

The first digit must be divisible by 4. For example: 0, 4, 8, ..., 252.

#### Attendant

When you select the 9641SIP template type from **Template**, the system enables the **Attendant** check box. If you select this check box, you can administer the endpoint as an attendant.

When you select the **Attendant** check box, the system disables the **Feature Options** and **Group Membership** tabs.

### Feature Options

With Features Options, you can set features unique to a particular voice terminal type.

#### Bridged Call Alerting

Controls how the user is alerted to incoming calls on a bridged appearance.

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | The bridged appearance rings when a call arrives at the primary telephone.                                                                                                                                                                                                                                    |
| n           | The bridged appearance flashes but does not ring when a call arrives at the primary telephone. This is the default.<br><br>If disabled and <b>Per Button Ring Control</b> is also disabled, audible ringing is suppressed for incoming calls on bridged appearances of another telephone's primary extension. |

#### Location

The system displays this field only when you set the **Multiple Locations** field on the system parameters customer options screen to y, and set the **Type** field to H.323 or SIP station types.

| Valid entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 to 2000   | (Depending on your server configuration, see <i>Avaya Aura® Communication Manager System Capacities Table</i> .) Assigns the location number to a particular station. Allows IP telephones and softphones connected through a VPN to be associated with the branch an employee is assigned to. This field is one way to associate a location with a station. For the other ways and for a list of features that use location, see the Location sections in <i>Avaya Aura® Communication Manager Feature Description and Implementation</i> . |
| blank       | Indicates that the existing location algorithm applies. By default, the value is blank.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

#### Active Station Ringing

Defines how calls ring to the telephone when it is off-hook without affecting how calls ring at this telephone when the telephone is on-hook.

| Valid Entry    | Usage                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| continuous     | All calls to this telephone ring continuously.                                                                                                                                                      |
| single         | Calls to this telephone receive one ring cycle and then ring silently.                                                                                                                              |
| if-busy-single | Calls to this telephone ring continuously when the telephone is off-hook and idle. Calls to this telephone receive one ring cycle and then ring silently when the telephone is off-hook and active. |
| silent         | All calls to this station ring silently.                                                                                                                                                            |

## Auto Answer

In an Expert Agent Environment (EAS) environment, the auto answer setting for an Agent LoginID overrides the endpoint settings when the agent logs in. In EAS environments, the auto answer setting for the Agent LoginID can override a station's setting when an agent logs in.

| Valid entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all         | All ACD and non-ACD calls to an idle station cut through immediately. The agent cannot use automatic hands-free answer for intercom calls. With non-ACD calls, the station rings while the call is cut through. To prevent the station from ringing, activate the <b>ringer-off</b> feature button, provided the Allow Ringer-off with Auto-Answer feature is enabled for the system.                                  |
| acd         | Only ACD split, ACD skill, and direct agent calls cut through. Non-ACD calls to the station ring audibly.<br>For analog stations: <ul style="list-style-type: none"> <li>• Only the ACD split or skill calls and direct agent calls cut through.</li> <li>• Non-ACD calls receive busy treatment. If the station is active on an ACD call and a non-ACD call arrives, the agent receives call-waiting tone.</li> </ul> |
| none        | All calls to the station receive an audible ringing.                                                                                                                                                                                                                                                                                                                                                                   |
| icom        | The user can answer an intercom call from the same intercom group without pressing the intercom button.                                                                                                                                                                                                                                                                                                                |

## MWI Served User Type

Controls the auditing or interrogation of a served user's message waiting indicator (MWI).

| Valid Entries | Usage                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| fp-mwi        | The station is a served user of an fp-mwi message center.                                                                |
| qsig-mwi      | The station is a served user of a qsig-mwi message center.                                                               |
| sip-adjunct   | Used to audit message waiting lamps.                                                                                     |
| blank         | The served user's MWI is not audited or if the user is not a served user of either an fp-mwi or qsig-mwi message center. |

## Coverage After Forwarding

Governs whether an unanswered forwarded call is provided coverage treatment.

| Valid Entry | Usage                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------|
| y           | Coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters.    |
| n           | No coverage treatment is provided after forwarding regardless of the administered system-wide coverage parameters. |
| s(ystem)    | Administered system-wide coverage parameters determine treatment.                                                  |

## Per Station CPN - Send Calling Number

Determines Calling Party Number (CPN) information sent on outgoing calls from this station.

| Valid Entries | Usage                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| y             | All outgoing calls from the station deliver the CPN information as “Presentation Allowed.”                                     |
| n             | No CPN information is sent for the call.                                                                                       |
| r             | Outgoing non-DCS network calls from the station delivers the Calling Party Number information as “Presentation Restricted.”    |
| blank         | The sending of CPN information for calls is controlled by administration on the outgoing trunk group the calls are carried on. |

## Display Language

| Valid Entry                                             | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| english<br>french<br>italian<br>spanish<br>user-defined | The language that displays on stations.<br><br>Time of day is displayed in 24-hour format (00:00 - 23:59) for all languages except English, which is displayed in 12-hour format (12:00 a.m. to 11:59 p.m.).                                                                                                                                                                                                                                                                                                                                                                                                                |
| unicode                                                 | Displays English messages in a 24-hour format. If no Unicode file is installed, displays messages in English by default.<br><br> <b>Note:</b><br>Unicode display is only available for Unicode-supported telephones. Currently, 4610SW, 4620SW, 4621SW, 4622SW, 16xx, 96xx, 96x1, 9600-series telephones (Avaya one-X Deskphone Edition SIP R2 or later), and Avaya J100 Series IP Phones support Unicode display. Unicode is also an option for DP1020 (aka 2420J) and SP1020 (Toshiba SIP Phone) telephones when enabled for the system. |

## Personalized Ringing Pattern

Defines the personalized ringing pattern for the station. Personalized Ringing allows users of some telephones to have one of 8 ringing patterns for incoming calls. For virtual stations, this field dictates the ringing pattern on its mapped-to physical telephone.

L = 530 Hz, M = 750 Hz, and H = 1060 Hz

| Valid Entries | Usage                  |
|---------------|------------------------|
| 1             | MMM (standard ringing) |
| 2             | HHH                    |
| 3             | LLL                    |
| 4             | LHH                    |
| 5             | HHL                    |
| 6             | HLL                    |

*Table continues...*



| Valid Entries | Usage |
|---------------|-------|
| 7             | HLH   |
| 8             | LHL   |

### Map-to Station

The extension of a physical telephone used for calls to a virtual extension. Cannot be used with an xmobile, xdid or any other virtual extension.

This field is applicable only for the virtual endpoints.

### Hunt-to Station

The extension the system must hunt to for this telephone when the telephone is busy. You can create a station hunting chain by assigning a hunt-to station to a series of telephones.

### Remote Soft Phone Emergency Calls

Tells Communication Manager how to handle emergency calls from the IP telephone.

#### **Caution:**

An Avaya IP endpoint can dial emergency calls (for example, 911 calls in the U.S.). It only reaches the local emergency service in the Public Safety Answering Point area where the telephone system has local trunks. You cannot use an Avaya IP endpoint to dial to and connect with local emergency service when dialing from remote locations that do not have local trunks. Avoid using an Avaya IP endpoint to dial emergency numbers for emergency services when dialing from remote locations. Avaya Inc. is not responsible or liable for any damages resulting from misplaced emergency calls made from an Avaya endpoint. Your use of this product indicates that you have read this advisory and agree to use an alternative telephone to dial all emergency calls from remote locations. If you have questions about emergency calls from IP telephones, go to the Avaya Support website at <http://support.avaya.com>.

Available only if the station is an IP Softphone or a remote office station.

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| as-on-local | <p>If the emergency location extension that corresponds to this station's IP address is not administered (left blank), the value as-on-local sends the station emergency location extension to the Public Safety Answering Point (PSAP).</p> <p>If the administrator populates the IP address mapping with emergency numbers, the value as-on-local functions as follows:</p> <ul style="list-style-type: none"> <li>• If the station emergency location extension is the same as the IP address mapping emergency location extension, the value as-on-local sends the station's own extension to the Public Safety Answering Point (PSAP).</li> <li>• If the station emergency location extension is different from the IP address mapping emergency location extension, the value as-on-local sends the IP address mapping extension to the Public Safety Answering Point (PSAP).</li> </ul> |

*Table continues...*

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| block       | Prevents the completion of emergency calls. Use this entry for users who move around but always have a circuit-switched telephone nearby, and for users who are farther away from the server than an adjacent area code served by the same 911 Tandem office. When users attempt to dial an emergency call from an IP Telephone and the call is blocked, they can dial 911 from a nearby circuit-switched telephone instead.                                                                                                                                                                                                                                                                                                                                                                    |
| cesid       | Allows Communication Manager to send the CESID information supplied by the IP Softphone to the PSAP. The end user enters the emergency information into the IP Softphone.<br><br>Use this entry for IP Softphones with road warrior service that are near enough to the server that an emergency call reaches the PSAP that covers the softphone's physical location. If the server uses ISDN trunks for emergency calls, the digit string is the telephone number, provided that the number is a local direct-dial number with the local area code, at the physical location of the IP Softphone. If the server uses CAMA trunks for emergency calls, the end user enters a specific digit string for each IP Softphone location, based on advice from the local emergency response personnel. |
| option      | Allows the user to select the option (extension, block, or cesid) that the user selected during registration and the IP Softphone reported. This entry is used for extensions that can be swapped back and forth between IP Softphones and a telephone with a fixed location.<br><br>The user chooses between block and cesid on the softphone. A DCP or IP telephone in the office automatically selects the extension.                                                                                                                                                                                                                                                                                                                                                                        |

### Bridging Tone for This Extension

Allows you to enable or disable a single burst of tone when a station bridges on to the principal's call.

| Valid Entry | Usage                                                                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | Enables a single burst of tone when a station bridges on to the principal's call.                                                                                                                                                        |
| n           | Disables a single burst of tone when a station bridges on to the principal's call.<br><br>This is the default value for a new SIP station, or when a SIP station upgrades to Communication Manager 8.0 or later from a previous release. |

### Service Link Mode

Use this field to specify the duration of a service link connection. The service link is the combined hardware and software multimedia connection between an H.320 Desktop Video Conferencing (DVC) system and Communication Manager.

The service link is established when a user receives or makes a call during a multimedia, IP softphone, or IP telephone session.

| Valid entry | Usage                                                                                                                                                                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| as-needed   | For multimedia, IP softphone, and IP telephone users. The service link remains connected for 10 seconds after the user disconnects a call so that the user can immediately make or receive another call. After 10 seconds, the link is disconnected, and a new link must be established to make or receive a call. |
| permanent   | For call center agents who are constantly making or receiving calls during the multimedia, IP softphone, or IP telephone session. The service link remains connected for the entire duration of the session.                                                                                                       |

### Loss Group

| Valid Entry | Usage                                                                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 to 17     | Determines which administered two-party row in the loss plan applies to each station. Is not displayed for stations that do not use loss, such as x-mobile stations. |

### Speakerphone

Controls the behavior of speakerphones.

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1-way       | Indicates that the speakerphone listen-only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 2-way       | Indicates that the speakerphone is both talk and listen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| grp-listen  | With Group Listen, a telephone user can talk and listen to another party with the handset or headset while the telephone's two-way speakerphone is in the listen-only mode. Others in the room can listen, but cannot speak to the other party through the speakerphone. The person talking on the handset acts as the spokesperson for the group. Group Listen provides reduced background noise and improves clarity during a conference call when a group needs to discuss what is being communicated to another party.<br><br>Available only with 6400-series and 2420/2410 telephones. |
| none        | Not administered for a speakerphone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### LWC Reception

Use this field to specify the location where the system must store the LWC messages.

| Valid entry | Usage                                                                        |
|-------------|------------------------------------------------------------------------------|
| spe         | Use this option to store the LWC messages on Switch Processor Element (SPE). |
| none        | Use this option if you do not want to store the LWC messages.                |
| auxix       | Use this option to store the LWC messages on the voice messaging system.     |

### Survivable COR

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level has the calling ability of the ones above it.

Available for all analog and IP station types.

| Valid Entries | Usage                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| emergency     | This station can only be used to place emergency calls.                                                                                                                      |
| internal      | This station can only make intra-switch calls. This is the default.                                                                                                          |
| local         | This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.                                      |
| toll          | This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.                                  |
| unrestricted  | This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users. |

#### Time of Day Lock Table

| Valid Entry | Usage                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------|
| 1 to 5      | Assigns the station to a Time of Day (TOD) Lock/Unlock table. The assigned table must be administered and active. |
| blank       | Indicates no TOD Lock/Unlock feature is active. This is the default.                                              |

#### Survivable GK Node Name

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the Branch Gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. With this, the IP station can use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46xx or 96xx models.

#### Media Complex Ext

When used with Multi-media Call Handling, indicates which extension is assigned to the data module of the multimedia complex. Users can dial this extension to place either a voice or a data call, and voice conversion, coverage, and forwarding apply as if the call were made to the 1-number.

| Valid Entry                | Usage                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------|
| A valid BRI data extension | For MMCH, enter the extension of the data module that is part of this multimedia complex. |

*Table continues...*

| Valid Entry             | Usage                                                                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H.323 station extension | For 4600 series IP Telephones, enter the corresponding H.323 station. For IP Softphone, enter the corresponding H.323 station. If you enter a value in this field, you can register this station for either a road-warrior or telecommuter/Avaya IP Agent application. |
| blank                   | Leave this field blank for single-connect IP applications.                                                                                                                                                                                                             |

### AUDIX Name

The voice messaging system associated with the station. Must contain a user-defined adjunct name that was previously administered.

### Call Appearance Display Format

Specifies the display format for the station. Bridged call appearances are not affected by this field. This field is available only on telephones that support downloadable call appearance buttons, such as the 2420 and 4620 telephones.

 **Note:**

This field sets the administered display value only for an individual station.

| Valid Entry       | Usage                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------|
| loc-param-default | The system uses the administered system-wide default value. This is the default.                                 |
| inter-location    | The system displays the complete extension on downloadable call appearance buttons.                              |
| intra-location    | The system displays a shortened or abbreviated version of the extension on downloadable call appearance buttons. |

### IP Phone Group ID

Available for H.323 and SIP station types.

| Valid entry | Usage                                |
|-------------|--------------------------------------|
| 0 to 999    | The Group ID number for the station. |
| blank       |                                      |

### Configuration of IP Phone Group ID on SIP Devices

You can configure the **IP Phone Group ID** field for SIP endpoints on:

- System Manager web console by using one of the following pages:
  - **Elements > Communication Manager > Endpoints > New > Manage Endpoints > Feature Options.**
  - **User Management > Manage Users > New > Communication Profile > CM Endpoint Profile > Extension Editor > Feature Options.**
  - **Elements > Communication Manager > Element Cut-Through.**
- Communication Manager SAT, using the `add station` command on page 3 of the Station form.

- Endpoint using the **Group** field.

 **Note:**

If you manually set the **Group** field on the endpoint to a value other than 0, then the group setting on the endpoint takes precedence over the **IP Phone Group ID** setting on the System Manager web console or Communication Manager station form.

If you manually set the **IP Phone Group ID** field on the System Manager web console or Communication Manager station form to value 0, then the **Group** field setting on the endpoint takes precedence over the **IP Phone Group ID** setting.

If the assigned group ID is not defined as the **Terminal Group Number** on the **Elements > Session Manager > Device and Location Configuration > Device Settings Group** page, the system applies the **Default Group** settings that are defined on the **Elements > Session Manager > Device and Location Configuration > Device Settings Group** page.

For administering **Terminal Group Number**, see *Administering Avaya Aura® Session Manager*.

## Configuring the IP Phone Group ID for an endpoint

### About this task

Use one of the following procedures to configure the **IP Phone Group ID** field on the System Manager web console.

- Click **Elements > Communication Manager > Endpoints > Manage Endpoints**, and perform the following:
  1. Click **New**.  
The system displays the New Endpoint page.
  2. In the **Template** field, select the required template.
  3. In the **Extension** field, type the extension number.
  4. On the **Feature Options** tab, in the **IP Phone Group ID** field, type the group ID for the endpoint.

When you change the group ID of the endpoint, the system displays the following message:

Changes to this field may result in some or all the user's of Avaya SIP phones to reboot once they are not involved in a SIP call or in other important functions.

5. Click **Commit** to save the changes.
- Click **User Management > Manage Users**, and perform the following:
    1. Click **New**.  
The system displays the User Profile | Add page.
    2. On the **Identity** tab, fill the required details.

3. On the **Communication Profile** tab, in PROFILES, click **CM Endpoint Profile**.
4. In the **System** field, select the Communication Manager system.
5. In the **Profile Type** field, select **Endpoint**.
6. In the **Extension** field, type the extension number, and then click the **Editor** button next to the given extension number.

System Manager displays the Edit Endpoint window.

7. In the **Template** field, select the required endpoint template.
8. On the **Feature Options** tab, in the **IP Phone Group ID** field, type the group ID for the endpoint.

When you change the group ID of the endpoint, the system displays the following message:

Changes to this field may result in some or all the user's of Avaya SIP phones to reboot once they are not involved in a SIP call or in other important functions.

9. Click **Commit** to save the changes.

### Next steps

Configure the **Terminal Group Number** field on the **Elements > Session Manager > Device and Location Configuration > Device Settings Group** page.

For administering **Terminal Group Number**, see *Administering Avaya Aura® Session Manager*.

### Always Use

Use this field to enable the following emergency call handling settings:

- A softphone can register irrespective of the emergency call handling settings the user has entered into the softphone. If a softphone dials 911, the value administered in the **Emergency Location Extension** field is used as the calling party number. The user-entered emergency call handling settings of the softphone are ignored.
- If an IP telephone dials 911, the value administered in the **Emergency Location Extension** field is used as the calling party number.
- If an agent dials 911, the physical station extension is used as the calling party number, overriding the value administered in the **LoginID for ISDN Display** field.

Does not apply to SCCAN wireless telephones, or to extensions administered as type H.323.

### Audible Message Waiting

Audible Message Waiting field enables or disables an audible message waiting tone indicating the user has a waiting message consisting of a stutter dial tone when the user goes off-hook.

This field does not control the Message Waiting lamp.

Available only if **Audible Message Waiting** is enabled for the system.

### Auto Select Any Idle Appearance

Auto Select Any Idle Appearance field enables or disables automatic selection of any idle appearance for transferred or conferenced calls. Communication Manager first attempts to find an idle appearance that has the same extension number as the call being transferred or conferenced has. If that attempt fails, Communication Manager selects the first idle appearance.

#### Bridged Idle Line Preference

Use this field to specify that the line that the system selects when you go off hook is always an idle call appearance for incoming bridged calls.

| Valid entry | Usage                                                                     |
|-------------|---------------------------------------------------------------------------|
| y           | The user connects to an idle call appearance instead of the ringing call. |
| n           | The user connects to the ringing bridged appearance.                      |

#### CDR Privacy

Enables or disables Call Privacy for each station. With CDR Privacy, digits in the called number field of an outgoing call record can be blanked on a per-station basis. The number of blocked digits is administered system-wide as CDR parameters.

#### Conf/Trans On Primary Appearance

Enables or disables the forced use of a primary appearance when the held call to be conferenced or transferred is a bridge. This is regardless of the administered value for **Auto Select Any Idle Appearance**.

#### Coverage Msg Retrieval

Allows or denies users in the telephone's Coverage Path to retrieve Leave Word Calling (LWC) messages for this telephone. Applies only if the telephone is enabled for LWC Reception.

#### IP Video

Use this field to specify whether the extension has IP video capability. The system displays this field for H.323 and SIP station types.

#### Data Restriction

Enables or disables data restriction that is used to prevent tones, such as call-waiting tones, from interrupting data calls. Data restriction provides permanent protection and cannot be changed by the telephone user. Cannot be assigned if **Auto Answer** is administered as all or acd. If enabled, whisper page to this station is denied.

#### Direct IP-IP Audio Connections

Use this field to enable direct audio connections between IP endpoints. Direct audio connections save bandwidth resources and improve the sound quality of voice over IP transmissions.

#### Display Client Redirection

Enables or disables the display of redirection information for a call originating from a station with Client Room Class of Service and terminating to this station. When disabled, only the client name and extension or room display. Available only if Hospitality is enabled for the system.



**\* Note:**

This field must be enabled for stations administered for any type of voice messaging that needs display information.

### Select Last Used Appearance

| Valid Entry | Usage                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y           | Indicates a station's line selection is not to be moved from the currently selected line button to a different, non-alerting line button. The line selection on an on-hook station only moves from the last used line button to a line button with an audibly alerting call. If there are no alerting calls, the line selection remains on the button last used for a call. |
| n           | The line selection on an on-hook station with no alerting calls can be moved to a different line button that might be serving a different extension.                                                                                                                                                                                                                        |

### Survivable Trunk Dest

Designates certain telephones as not being allowed to receive incoming trunk calls when the Branch Gateway is in survivable mode.

Available for all analog and IP station types.

| Valid Entry | Usage                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| y           | Allows this station to be an incoming trunk destination while the Branch Gateway is running in survivability mode. This is the default. |
| n           | Prevents this station from receiving incoming trunk calls when in survivable mode.                                                      |

### H.320 Conversion

Use this field to enable the conversion of H.320-compliant calls to voice-only calls for the attendant console.

**\* Note:**

The system can handle only a limited number of conversion calls. Therefore, the number of attendant consoles with H.320 conversion must be limited.

### Idle Appearance Preference

Indicates which call appearance is selected when the user lifts the handset and there is an incoming call.

| Valid Entry | Usage                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------|
| y           | The user connects to an idle call appearance instead of the ringing call.                       |
| n           | The Alerting Appearance Preference is set and the user connects to the ringing call appearance. |

### IP Audio Hairpinning

Enables or disables hairpinning for H.323 or SIP trunk groups. H.323 endpoints are connected through the IP circuit pack without going through the time division multiplexing (TDM) bus. Available only if **Group Type** is h.323 or sip.

#### IP Softphone

Indicates whether or not this extension is either a PC-based multifunction station or part of a telecommuter complex with a call-back audio connection.

Available only for DCP station types and IP Telephones.

#### LWC Activation

Activates or deactivates the Leave Word Calling (LWC) feature. With LWC, internal telephone users on this extension can leave short pre-programmed messages for other internal users.

You must use LWC if:

- The system has hospitality and the guest-room telephones require LWC messages indicating that wakeup calls failed
- The LWC messages are stored in a voice-messaging system

#### LWC Log External Calls

This field can be configured when the set type is XMOBILE. Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.

#### IP Hoteling

When you enable the **(SA8520) - Hoteling Application for IP Terminals** field using the **change system-parameters special-applications** command on Communication Manager, the system displays the **IP Hoteling** field for that extension.

Avaya supports this application with DCP digital terminals but not with IP terminals. Using this feature, you can reassign the extension number for a registered IP telephone.

For more information, see *Avaya Aura® Communication Manager Special Application Features*.

#### Multimedia Early Answer

Enables or disables multimedia early answer on a station-by-station basis.

You must enable the station for the Multimedia Early Answer feature if the station receives coverage calls for multimedia complexes, but is not multimedia-capable. This ensures that calls are converted and the talk path is established before ringing at this station.

#### Mute Button Enabled

Enables or disables the mute button on the station.

#### Per Button Ring Control

Using this option you can enable or disable ring control for every button, provided you have the station user credentials.

| Valid Entries | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| y             | <p>To enable Automatic Abbreviated and Delayed ring transition for each call-appr on the station, select ring behavior individually for each call-appr or brdg-appr option.</p> <p>To prevent the system from automatically moving the line selection to a silently alerting call, unless the call was audibly ringing earlier.</p> <p> <b>Note:</b></p> <p>The abrdg-appr option is unavailable for SIP station.</p> |
| n             | <p>To enable the calls on <b>call-appr</b> buttons always to ring the station</p> <p>To enable the calls on <b>brdg-appr</b> buttons always ring or not ring based on the <b>Bridged Call Alerting</b> value</p> <p>To move line selection to a silently alerting call, if the call is not audibly ringing the station</p> <p> <b>Note:</b></p> <p>The abrdg-appr option is unavailable for SIP station.</p>          |

### Precedence Call Waiting

Activates or deactivates Precedence Call Waiting for this station.

### Redirect Notification

Enables or disables redirection notification that gives a half ring at this telephone when calls to this extension are redirected through Call Forwarding or Call Coverage. Must be enabled if LWC messages are stored on a voice-messaging system.

### Restrict Last Appearance

| Valid Entries | Usage                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------|
| y             | Restricts the last idle call appearance used for incoming priority calls and outgoing call originations only. |
| n             | Last idle call appearance is used for incoming priority calls and outgoing call originations.                 |

### EMU Login Allowed

Enables or disables using the station as a visited station by an Enterprise Mobility User (EMU).

### Bridged Appearance Origination Restriction

Restricts or allows call origination on the bridged appearance.

| Valid Entry | Usage                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------|
| y           | Call origination on the bridged appearance is restricted.                                           |
| n           | Call origination on the bridged appearance is allowed. This is normal behavior, and is the default. |

### Voice Mail Number

Displays the complete voice mail dial up number. Accepts a value of up to 24 characters consisting of digits from 0 to 9, asterisk (\*), pound sign (#), ~p (pause), ~w/~W (wait), ~m (mark), and ~s (suppress). This field is supported in the following set types: 9620SIP, 9630SIP, 9640SIP, 9650SIP, 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, and 9641SIPCC.

#### Music Source

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Music Source</b> | <p>Valid values are 1 to 100 or blank. The value can extend to 250 when you select the Multi Tenancy feature from the system parameter customer option on the Communication Manager.</p> <p><b>Music Source</b> field is applicable for all endpoint set types.</p> <p> <b>Note:</b></p> <p>Select the <b>System Parameter Special Application</b>, and select <b>SA8888 Per Station Music On Hold</b>, Only then you can select the <b>Music source</b> field.</p> |

#### Site Data

This section lets you set information about the Room, Floor, Jack, Cable, Mounting, and Building.

#### Room

| Valid Entry               | Usage                                                                                                                                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Telephone location</i> | Identifies the telephone location. Accepts up to 10 characters.                                                                                                                                              |
| <i>Guest room number</i>  | Identifies the guest room number if this station is one of several to be assigned a guest room and the <b>Display Room Information in Call Display</b> is enabled for the system. Accepts up to five digits. |

#### Floor

A valid floor location.

#### Jack

Alpha-numeric identification of the jack used for this station.

#### Cable

Identifies the cable that connects the telephone jack to the system.

#### Mounting

Indicates whether the station mounting is d(esk) or w(all).

#### Building

A valid building location.

#### Set Color

Indicates the set color. Valid entries include the following colors: beige, black, blue, brown, burg (burgundy), gray, green, ivory, orng (orange), red, teak, wal (walnut), white, and yel (yellow).

You can change the list of allowed set colors by using the Valid Set Color fields on the site-data screen.

#### Cord Length

The length of the cord attached to the receiver. This is a free-form entry, and can be in any measurement units.

#### Headset

Indicates whether or not the telephone has a headset.

#### Speaker

Indicates whether or not the station is equipped with a speaker.

### **Abbreviated Call Dialing**

This section lets you create abbreviated dialing lists for a specific station, and provide lists of stored numbers that can be accessed to place local, long-distance, and international calls; allows you to activate features or access remote computer equipment and select enhanced, personal, system or group lists.

#### Abbreviated Dialing List 1, List 2, List 3

Assigns up to three abbreviated dialing lists to each telephone.

| Valid Entry | Usage                                                                                                                             |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------|
| enhanced    | Telephone user can access the enhanced system abbreviated dialing list.                                                           |
| group       | Telephone user can access the specified group abbreviated dialing list. Requires administration of a group number.                |
| personal    | Telephone user can access and program their personal abbreviated dialing list. Requires administration of a personal list number. |
| system      | Telephone user can access the system abbreviated dialing list.                                                                    |

#### Personal List

Use this list to establish a personal dialing list for telephone or data module users.

#### Enhanced List

Use this list to establish system-wide or personal lists for speed dialing.

Users access this list to:

- place local, long-distance, and international calls
- activate or deactivate features
- access remote computer equipment.

#### **Note:**

You must activate dialing in the license file before the system programs the Abbreviated Dialing Enhanced List.

#### Group List

You can provide up to 100 numbers for every group list.

## Enhanced Call Fwd

This section allows you to specify the destination extension for the different types of call forwards.

### Forwarded Destination

A destination extension for both internal and external calls for each of the three types of enhanced call forwarding (Unconditional, Busy, and No Reply). Accepts up to 18 digits. The first digit can be an asterisk \*.

Requires administration to indicate whether the specific destination is active (enabled) or inactive (disabled).

### SAC/CF Override

With **SAC/CF Override**, the user of the calling station can override the redirection set by the called station.

| Valid entry | Usage                                                                                                                                                            |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ask         | The system prompts the user of the calling station whether the call must follow the redirection path or override the redirection path. The user can type y or n. |
| no          | The user of the calling station cannot override the redirection path of the call. The call follows the redirection path.                                         |
| yes         | The user of the calling station can override the redirection path of the call, provided the called station has at least one idle call appearance.                |

## Button Assignment

On the Manage Endpoints page, under the **Button Assignment** tab, the system displays the following tabs based on the **Set Type** selection:

- **Main Buttons**
- **Feature Buttons**
- **Buttons Modules**
- **Phone View**

### \* Note:

With System Manager Release 8.1.1, the **Phone View** tab is displayed for SIP Endpoints.

You can assign features to the buttons on a phone. You can assign the main buttons for your endpoint by choosing an option from the list for each button.

### \* Note:

On the Manage Endpoint page, when you select the CS 1000 station type and specific set from the **Set** field, System Manager enables or disables the options on **Button Assignment** according to the selected set of the CS 1000 station type.

## Field descriptions

### Endpoint Configurations:

The Favorite Button and Button Label configurations are available on the 9608, 9611, 9621, 9641 SIP, 96x1SIPCC, J-Series, and CS 1000 endpoints.

The Favorite Button and Button Label features function when the endpoint is associated to a user with the Session Manager profile.

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Favorite</b>     | <p>The favorite button.</p> <p> <b>Note:</b></p> <p>You can mark maximum nine buttons as favorites on an endpoint, which includes the configured contacts on the phone.</p> <p>The <b>Favorite</b> button is disabled for the <b>call-app</b> and <b>bridge-app</b> button features. Therefore, you cannot select these button features as a favorite.</p> <p>To set the <b>Auto Dial</b> button as a favorite, or to set <b>Button Label</b> for auto dial, you must specify the <b>Dial Number</b>.</p> |
| <b>Button Label</b> | <p>The personalized button label that is displayed on the phone.</p> <p> <b>Note:</b></p> <p>The button label is not localized on the phone.</p>                                                                                                                                                                                                                                                                                                                                                          |

#### Button Configurations:

| Name                                    | Description                                                         |
|-----------------------------------------|---------------------------------------------------------------------|
| <b>Button Number on Phone</b>           | The button number that is available on the phone.                   |
| <b>Button Number Administered in CM</b> | The button number that is administered on Communication Manager.    |
| <b>Button Feature or Feature</b>        | The button feature that is available on the phone.                  |
| <b>Argument</b>                         | The argument for the button feature that is available on the phone. |

#### Phone view layout of SIP Endpoints

With System Manager Release 8.1.1, you can view the read only phone view layout of SIP Endpoints when the SIP endpoint is registered with Session Manager.

The **Phone View** tab displays the data based on the **Set Type** configuration on the Manage Endpoints page. It is supported only for the following SIP endpoints: J1xx, 96x1 SIP, and 96x0 SIP set types.

The system displays the tabular layout of feature buttons based on the key number ordering of the endpoint.

If the endpoint supports the following two button types, the **Phone View** tab also displays the data about these buttons, if they are configured.

- Contact name on the endpoint then text **Contact** is displayed on phone view instead of the actual contact name available in the customize key on the endpoint.

Example: If the key layout customization contains Calendar, its App on the endpoint, then on the **Phone View** tab, the value is displayed as **Calendar (App)**.

- App (Application) on the endpoint then **App** is appended to key layout customization while displaying on the phone view.

**Endpoints that support key layout customization**

- If the endpoints support the key layout customization, then the phone key numbering is displayed on **Phone View** as customized by the user on the endpoint.

| General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P) Group Membership (M) |                                  |                |          |            |            |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------|----------|------------|------------|------------|
| Main Buttons Feature Buttons Button Modules Phone View                                                                                                                     |                                  |                |          |            |            |            |
| Button Number on Phone                                                                                                                                                     | Button Number Administered in CM | Feature        | Label    | Argument-1 | Argument-2 | Argument-3 |
| 1                                                                                                                                                                          | 1                                | call-appr      |          |            |            |            |
| 2                                                                                                                                                                          | 2                                | call-appr      |          |            |            |            |
| 3                                                                                                                                                                          | 3                                | call-appr      |          |            |            |            |
| 4                                                                                                                                                                          | ---                              | Calendar (App) | Calendar |            |            |            |
| 5                                                                                                                                                                          | ---                              | Log Out (App)  |          |            |            |            |
| 6                                                                                                                                                                          | ---                              | Contact        |          |            |            |            |
| 7                                                                                                                                                                          |                                  |                |          |            |            |            |
| 8                                                                                                                                                                          |                                  |                |          |            |            |            |

- If the endpoint is not registered with Session Manager or data is not available with Session Manager, then the system displays the message: Phone View Data not Available

System

psm-cm95

Extension

40006

Template

Select

Set Type

J179

Port

S000008

Security Code

\*\*\*\*\*

Name

Bah

General Options (G) \* Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

Main Buttons Feature Buttons Button Modules Phone View

Phone View Data not Available

\* Required

**Endpoints that do not support key layout customization**

If the endpoints do not support the key layout customization, then the phone key numbering is displayed as administered on Communication Manager.

Examples of endpoints that do not support the key layout customization are: J129, J139, 9641SIP, and 9641SIPCC.



General Options (G) \*Feature Options (F)Site Data (S)Abbreviated Call Dialing (A)Enhanced Call Fwd (E)Button Assignment (B)Profile Settings (P)

Group Membership (M)

Main ButtonsFeature ButtonsButton ModulesPhone View

| Button Number Administered in CM | Feature   | Label | Argument-1   | Argument-2 | Argument-3 |
|----------------------------------|-----------|-------|--------------|------------|------------|
| 1                                | call-appr |       |              |            |            |
| 2                                | call-appr |       |              |            |            |
| 3                                | call-appr |       |              |            |            |
| 4                                | ec500     |       | Timer?n      |            |            |
| 9                                | busy-ind  |       | TAC/Ext40006 |            |            |

Button Module 1

|   |            |  |  |  |  |
|---|------------|--|--|--|--|
| 1 | crss-alert |  |  |  |  |
|---|------------|--|--|--|--|

Button Module 2

|   |           |  |  |  |  |
|---|-----------|--|--|--|--|
| 1 | call-park |  |  |  |  |
|---|-----------|--|--|--|--|

\*Required

CommitScheduleResetCancel

Endpoint display mode

The phone can be set to use either the full screen width (single-column mode) or just a half-width (dual-column mode) for each programmable appearance and feature button.

Full screen width (single-column mode)

Each programmed button feature occupies the full width of the screen. The physical buttons on both sides of the display are used to control the button feature. However, the button status is only shown by the left-hand button. In this mode, appearance button labels also show a call status icon (for example: idle, alerting, connected).

Following is an example of endpoint display mode in full screen width.

The number in the following example corresponds to the **Button Number on Phone** column on the **Phone View** tab of the Add/Edit Endpoint page.

1  
2  
3  
4  
5  
.  
.  
.  
<n>

The number in the following table corresponds to the **Button Number on Phone** column on the **Phone View** tab of the Endpoint page.

Half-width (dual-column mode)

Each programmed button occupies one half of the screen line on which it is displayed, either the right-hand or left-hand side. The adjacent physical button on that side of the display is used to indicate the button's status and to control the button feature.

Following is an example of endpoint display mode in half-width screen.

The number in the following example corresponds to the **Button Number on Phone** column on the **Phone View** tab of the Add/Edit Endpoint page.

|   |     |
|---|-----|
| 1 | 2   |
| 3 | 4   |
| 5 | 6   |
| 7 | 8   |
| . | .   |
| . | .   |
| . | <n> |

### Profile settings field descriptions

#### \* Note:

Profile Settings is available for the 9608, 9611, 9621, 9641 SIP, 96x1SIPCC, J-Series, and CS 1000 endpoints.

Profile Settings work when the endpoint is associated to a user with a Session Manager profile.

### Call Settings options

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Phone Screen on Calling</b> | The option to specify whether the phone must automatically display the phone screen when the user goes off-hook or starts dialing. The options are: <ul style="list-style-type: none"> <li>• <b>Yes.</b></li> <li>• <b>No.</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Redial</b>                  | The field to select from the following redial options: <ul style="list-style-type: none"> <li>• <b>List:</b> To display a list of recently dialed numbers.</li> <li>• <b>One Number:</b> To automatically dial the last dialed number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Dialing Option</b>          | The field to specify the dialing options: <ul style="list-style-type: none"> <li>• <b>Editable:</b> To enable off-hook dialing that mimics dialing a call on a cell phone. When the user starts dialing, the edit dialing interface displays the dialed digits. The user can enter all or part of the number or backspace to correct a number if needed. When ready, the user must press the <b>Call</b> soft key to connect.</li> <li>• <b>On-hook:</b> To enable on-hook dialing so that when the user starts dialing, the phone automatically goes on-hook on the first available line and dials the digits.</li> </ul> |
| <b>Headset Signaling</b>       | The field that defines a headset signaling profile. The options are: <ul style="list-style-type: none"> <li>• <b>Disabled:</b> To disable headset signaling profile.</li> <li>• <b>Switchhook and Alerts:</b> To set the switch hook and alert headset signaling profile.</li> <li>• <b>Switchhook only:</b> To set the switch hook headset signaling profile.</li> </ul>                                                                                                                                                                                                                                                  |

*Table continues...*

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Audio Path</b> | <p>The field to set the phone to go off-hook when you make an on-hook call. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Speaker:</b> To go off-hook on the Speaker when you make an on-hook call.</li> <li>• <b>Headset:</b> To go off-hook on the Headset when you make an on-hook call.</li> </ul> <p> <b>Note:</b></p> <p>If your system administrator has set up auto-answer, incoming calls are also answered on the default audio path you designate here.</p> |

### Screen & Sound Options

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Button Clicks</b>   | <p>The field to activate or deactivate the standard button click sound. The options are:</p> <ul style="list-style-type: none"> <li>• <b>On.</b></li> <li>• <b>Off.</b></li> </ul>                                                                                                                                                                                                                    |
| <b>Phone Screen</b>    | <p>The field to configure the phone screen width. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Half:</b> To split the phone screen width to half so that each call appearance or feature occupies half the width of a line.</li> <li>• <b>Full:</b> To set the phone screen width to full so that each call appearance or feature occupies the entire width of a line.</li> </ul> |
| <b>Background Logo</b> | <p>The option to set a customized background logo. The <b>Default</b> value sets the built-in Avaya logo.</p>                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personalized Ringing</b>   | <p>The option to set a personalized ring tone for an incoming call. The options are:</p> <ul style="list-style-type: none"> <li>• Classic Tone, with 8 options</li> <li>• Cheerful</li> <li>• Chimes</li> <li>• Telephone Bell</li> <li>• Xylophone</li> <li>• Drum Beat</li> <li>• Shimmer</li> </ul> <p> <b>Note:</b></p> <p>The Personalized Ringing parameter is available on the Communication Manager Release 6.2 and 6.3 templates.</p> <p>However, the parameter does not apply to Release 6.2 and earlier Avaya Advanced SIP Telephony (AST) endpoints. In some cases, the Avaya EST endpoints might overwrite the newly configured value of the parameter. For example, an endpoint where the related ringing parameter called Ringer Cadence is set to a value other than 1. In this case, the endpoint sets the Personalized Ringing parameter to the value of Ringer Cadence within a few minutes of the change. The reset can also happen during the next login of the endpoint.</p> <p>Session Manager was modified to reduce the instances of this occurrence. The default value of Ringer Cadence is set to 1 for any new Device Settings Groups added to Release 6.3.8.</p> <p>You can set the parameter on the <b>Device and Location Configuration &gt; Device Settings Groups</b> page from the <b>Elements &gt; Session Manager</b> link.</p> |
| <b>Call Pickup Indication</b> | <p>The option to set ring tones to alert you about an incoming call. The options are:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> No pickup indication for an incoming call.</li> <li>• <b>Audible:</b> Audible ringing indicates an incoming call.</li> <li>• <b>Visual:</b> LED flashes indicate an incoming call.</li> <li>• <b>Both:</b> Both audible ringing and LED flashes indicate an incoming call.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Show Quick Touch Panel</b> | <p>The options to display <b>Quick Touch Panel</b> on the phone. The options are:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Not to display <b>Quick Touch Panel</b>.</li> <li>• <b>1</b>: To display a one-line <b>Quick Touch Panel</b>.</li> <li>• <b>2</b>: To display a two—line <b>Quick Touch Panel</b>.</li> </ul> <p> <b>Note:</b></p> <p>Displaying the <b>Quick Touch Panel</b> field can limit your call appearances display to three lines at a time.</p> <p>This field is available for 9621 and 9641 SIP, and SIPCC set type of endpoints.</p> |

## Language & Region

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Language</b> | <p>The option to configure the language. The options are:</p> <ul style="list-style-type: none"> <li>• English</li> <li>• Hebrew</li> <li>• Brazilian Portuguese</li> <li>• Canadian French</li> <li>• German</li> <li>• Parisian French</li> <li>• Latin American Spanish</li> <li>• Castilian Spanish</li> <li>• Italian</li> <li>• Dutch</li> <li>• Russian</li> <li>• Simplified Chinese</li> <li>• Japanese</li> <li>• Korean</li> <li>• Arabic</li> </ul> <p> <b>Note:</b></p> <p>The Arabic language is not available for 9608 SIP and SIPCC set type of endpoints.</p> |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Preferred Language</b> | <p>The option to configure the user preferred language. The options are:</p> <ul style="list-style-type: none"> <li>• English</li> <li>• Hebrew</li> <li>• Brazilian Portuguese</li> <li>• Canadian French</li> <li>• German</li> <li>• Parisian French</li> <li>• Latin American Spanish</li> <li>• Castilian Spanish</li> <li>• Italian</li> <li>• Dutch</li> <li>• Russian</li> <li>• Simplified Chinese</li> <li>• Japanese</li> <li>• Korean</li> <li>• Arabic</li> </ul> <p> <b>Note:</b></p> <p>The Arabic language is not available for 9608 SIP and SIPCC set type of endpoints.</p> |

*Table continues...*

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Language File in Use</b> | <p>The option to configure the file name to use for the configured language. The options are:</p> <ul style="list-style-type: none"> <li>• Mlf_English.xml</li> <li>• Mlf_Hebrew.xml</li> <li>• Mlf_BrazilianPortuguese.xml</li> <li>• Mlf_CanadianFrench.xml</li> <li>• Mlf_German.xml</li> <li>• Mlf_ParisianFrench.xml -</li> <li>• Mlf_LatinAmericanSpanish.xml</li> <li>• Mlf_CastilianSpanish.xml</li> <li>• Mlf_Italian.xml</li> <li>• Mlf_Dutch.xml</li> <li>• Mlf_Russian.xml</li> <li>• Mlf_Chinese.xml</li> <li>• Mlf_Japanese.xml</li> <li>• Mlf_Korean.xml</li> <li>• Mlf_Arabic.xml</li> </ul> <p> <b>Note:</b></p> <p>The Mlf_Arabic.xml language file is not available for 9608 SIP and SIPCC set type of endpoints.</p> |
| <b>Time Format</b>          | <p>The option to configure the time format to be displayed on the phone screen. The options are:</p> <ul style="list-style-type: none"> <li>• <b>12 Hour.</b></li> <li>• <b>24 Hour.</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### Advance Options Presence integration

| Name               | Description                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Away Timer</b>  | <p>The option to enable the automatic away timer for presence indication. The options are:</p> <ul style="list-style-type: none"> <li>• <b>On.</b></li> <li>• <b>Off.</b></li> </ul> |
| <b>Timer Value</b> | <p>The option to specify a value for the automatic <b>Away Timer</b>. The <b>Timer Value field</b> accepts a value from 5 to 480.</p>                                                |

Support of common parameter across endpoint template

With Release 8.1.1, when you create a SIP endpoint, the system retains the common parameter information so that when you log in to SIP endpoints of the same type or of another type, all your SIP endpoints are able to retrieve and update any of the common parameters they utilize.

The following common parameters are available on the **Profile Settings** tab on the **Elements > Communication Manager > Endpoints > Manage Endpoints** page of System Manager web console.

- **Audio Path**
- **Away Timer**
- **Away Timer Value**
- **Background Logo**
- **Button Clicks**
- **Call Pickup Indication**
- **Dialing Option**
- **Headset Signaling**
- **Personalized Ringing**
- **Phone Screen**
- **Phone Screen on Calling**
- **Redial**
- **Show Quick Touch Panel**
- **Time Format**
- **User Preferred Language**

The following common parameters are available on the **Button Assignment** tab on the **Elements > Communication Manager > Endpoints > Manage Endpoints** page of System Manager web console.

- **Favorite**
- **Button Label**

 **Note:**

- When you make changes to a common parameter from System Manager, the system gives precedence to that value as System Manager values are from a well-defined common parameter range. But when you make changes to a common parameter from an endpoint, the system gives precedence to that value only if the value is from the well-defined common parameter range. If the value is not from the well-defined common parameter range, then the value is only stored for that device family and the common value for that parameter is not changed.
- Family-specific data is not changed.

If you have more than one SIP endpoint type, the following parameters are synchronized across all your SIP endpoints, which support these parameters according to the following table.



| Common parameters       | 1XC<br>Model:<br>n/a | 96x0<br>Model:<br>96xx | 96x1<br>Model:<br>: 96x1 | J1x9<br>Model:<br>J100 | ADA<br>Model:<br>CS1k-<br>xxx | Equinox<br>Model:<br>AvayaClient<br>Services | Vantage<br>Model:<br>K1xx | H Series<br>Model:<br>H1xx, H175 |
|-------------------------|----------------------|------------------------|--------------------------|------------------------|-------------------------------|----------------------------------------------|---------------------------|----------------------------------|
| Audio Path              | Y                    | Y                      | Y                        | Y                      |                               |                                              |                           | Y                                |
| Away Timer              |                      |                        | Y                        | Y                      |                               |                                              |                           |                                  |
| Away Timer Value        |                      |                        | Y                        | Y                      |                               |                                              |                           |                                  |
| Background Logo         | Y                    | Y                      | Y                        |                        |                               |                                              |                           |                                  |
| Button Clicks           |                      | Y                      | Y                        | Y                      |                               |                                              | Y                         | Y                                |
| Call Pickup Indication  | Y                    |                        | Y                        | Y                      |                               |                                              |                           | Y                                |
| Dialing Option          |                      | Y                      | Y                        | Y                      |                               |                                              |                           | Y                                |
| Favorite                | Y                    | Y                      | Y                        | Y                      |                               |                                              |                           |                                  |
| Headset Signaling       |                      |                        | Y                        | Y                      |                               |                                              | Y                         | Y                                |
| Button Label            | Y                    | Y                      | Y                        | Y                      | Y                             | Y                                            |                           |                                  |
| Personalized Ringing    |                      |                        | Y                        | Y                      |                               |                                              |                           | Y                                |
| Phone Screen            |                      |                        | Y                        | Y                      |                               |                                              |                           |                                  |
| Phone Screen on Calling |                      | Y                      | Y                        |                        |                               |                                              |                           |                                  |
| Redial                  |                      |                        | Y                        | Y                      |                               |                                              |                           | Y                                |
| Show Quick Touch Panel  |                      | Y                      | Y                        |                        |                               |                                              |                           |                                  |
| Time Format             |                      |                        | Y                        | Y                      |                               |                                              | Y                         | Y                                |
| User Preferred Language |                      | Y                      | Y                        | Y                      |                               |                                              | Y                         | Y                                |

### Group Membership

This section describes the different groups that an extension can be a member of. Select the station you want to group, and then choose the group from the drop-down box, before you click **Commit**.

#### Understanding groups

Your voice system uses groups for a number of different purposes. This topic describes the different groups that an extension can be a member of. However, your voice system might include other types of groups such as trunk groups. For more information on groups, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Your voice system can have any of the following types of groups set up:

| Type                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| group page            | Group page is a feature that allows you to make an announcement to a pre-programmed group of phone users. The announcement is heard through the speakerphone built into some sets. Users will hear the announcement if their set is idle. Users cannot respond to the announcement.                                                                                                                                                                                                |
| coverage answer group | A coverage answer group lets up to 100 phones ring simultaneously when a call is redirected to the group.                                                                                                                                                                                                                                                                                                                                                                          |
| coverage path         | <p>A coverage path is a prioritized sequence of extensions to which your voice system will route an unanswered call.</p> <p>For more information on coverage paths, see “Creating Coverage Paths” in the <i>Administering Avaya Aura® Communication Manager, 03-300509</i>.</p>                                                                                                                                                                                                    |
| hunt group            | <p>A hunt group is a group of extensions that receive calls according to the call distribution method you choose. When a call is made to a certain phone number, the system connects the call to an extension in the group. Use hunt groups when you want more than one person to be able to answer calls to the same number.</p> <p>For more information on hunt groups, see “Managing Hunt Groups” in the <i>Administering Avaya Aura® Communication Manager, 03-300509</i>.</p> |
| intercom group        | <p>An intercom group is a group of extensions that can call each other using the intercom feature. With the intercom feature, you can allow one user to call another user in a predefined group just by pressing a couple of buttons.</p> <p>For more information on intercom groups, see “Using Phones as Intercoms” in the <i>Administering Avaya Aura® Communication Manager, 03-300509</i>.</p>                                                                                |
| pickup group          | <p>A pickup group is a group of extensions in which one person can pick up calls of another person.</p> <p>For more information on pickup groups, see “Adding Call Pickup” in the <i>Administering Avaya Aura® Communication Manager, 03-300509</i>.</p>                                                                                                                                                                                                                           |

Table continues...

| Type                        | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| terminating extension group | <p>A Terminating Extension Group (TEG) allows an incoming call to ring as many as 4 phones at one time. Any user in the group can answer the call.</p> <p>For more information on terminating extension groups, see “Assigning a Terminating Extension Group” in the <i>Administering Avaya Aura® Communication Manager</i>, 03-300509.</p> |

## Edit Endpoint Extension field descriptions

| Name                                    | Description                                                           |
|-----------------------------------------|-----------------------------------------------------------------------|
| <b>System</b>                           | The list of Communication Manager systems from where you can select.  |
| <b>Extension</b>                        | The extension of the device that you want to change.                  |
| <b>New Extension</b>                    | The new extension for the device.                                     |
| <b>Emergency location extension</b>     | The existing extension for the emergency location of your device.     |
| <b>New emergency location extension</b> | The new extension for the existing emergency location of your device. |
| <b>Message lamp extension</b>           | The existing extension for the message lamp of your device.           |
| <b>New message lamp extension</b>       | The new extension for the message lamp of your device.                |

| Button          | Description                                |
|-----------------|--------------------------------------------|
| <b>Commit</b>   | Saves the new extension.                   |
| <b>Schedule</b> | Saves the extension at the scheduled time. |
| <b>Reset</b>    | Clears all entries.                        |
| <b>Cancel</b>   | Returns to the previous page.              |

## Bulk Add Endpoint field descriptions

| Name                        | Description                                                              |
|-----------------------------|--------------------------------------------------------------------------|
| <b>Template</b>             | The template for the endpoints.                                          |
| <b>Station name prefix</b>  | The prefix name that the system displays for each endpoint that you add. |
| <b>System</b>               | The list of Communication Manager systems.                               |
| <b>Available extensions</b> | The list of extensions that are available.                               |
| <b>Enter extensions</b>     | The extensions that you want to use.                                     |

| Button          | Description                                     |
|-----------------|-------------------------------------------------|
| <b>Commit</b>   | Adds the endpoints in bulk.                     |
| <b>Schedule</b> | Adds the station in bulk at the scheduled time. |

Table continues...

| Button | Description                   |
|--------|-------------------------------|
| Clear  | Undoes all entries.           |
| Cancel | Returns to the previous page. |

## Swap Endpoints field descriptions

| Name                                      | Description                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assign data for Endpoint &lt;n&gt;</b> | An option to assign new values of location site data to an endpoint.<br><br>When you select this check box for an endpoint, the system copies the location site data values of this endpoint to the second endpoint where this check box is clear. If you select the check boxes for both endpoints, the system copies new location site data to respective endpoints. The system does not swap values. |
| <b>System</b>                             | Communication Manager to which the endpoint is assigned. The system is listed in the Communication Manager List page.                                                                                                                                                                                                                                                                                   |
| <b>Endpoint 1</b><br><b>Endpoint 2</b>    | The existing endpoint extension number on the selected Communication Manager.                                                                                                                                                                                                                                                                                                                           |

| Button   | Description                                                   |
|----------|---------------------------------------------------------------|
| Commit   | Performs the action that you initiate.                        |
| Schedule | Performs the action at the specified time.                    |
| Cancel   | Cancels your current action and returns to the previous page. |

## Error codes

The following table lists only the common error codes for Busyout, Release, Test, and Reset commands lists.

In addition to these, many maintenance objects have other unique error codes. For information about the applicable maintenance object, see *Avaya Aura® Communication Manager Alarms, Events, and Logs Reference*.

| Error code | Command result | Description/Recommendation                                                                                                                                                                                                                                |
|------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | ABORT          | System resources are unavailable to run command. Try the command again at 1-minute intervals up to 5 times.                                                                                                                                               |
| 0          | ABORT          | Internal system error. Retry the command at 1-minute intervals up to 5 times.                                                                                                                                                                             |
| 1005       | ABORT          | A DS1 interface circuit pack could not be reset because it is currently supplying the on-line synchronization reference. Use <b>set synchronization</b> to designate a new DS1 interface circuit pack as the on-line reference, then try the reset again. |
| 1010       | ABORT          | Attempt was made to busyout an object that was already busied out.                                                                                                                                                                                        |
| 1011       | ABORT          | Attempt was made to release an object that was not first busied out.                                                                                                                                                                                      |

*Table continues...*

| Error code              | Command result | Description/Recommendation                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1015                    | ABORT          | A reset of this circuit pack requires that every maintenance object on it be in the out-of-service state. Use busyout board to place every object on the circuit pack in the out-of-service state, and try the reset again.                                                                                                                                                                                                       |
| 1026                    | ABORT          | The specified TDM bus cannot be busied out because the control channel or system tones are being carried on it. Use <code>set tdm PC</code> to switch the control channel and system tones to the other TDM bus.                                                                                                                                                                                                                  |
| 2012 2500               | ABORT          | Internal system error.                                                                                                                                                                                                                                                                                                                                                                                                            |
| 2100                    | ABORT          | System resources to run this command were unavailable. Try the command again at 1-minute intervals up to 5 times.                                                                                                                                                                                                                                                                                                                 |
| 62524<br>62525<br>62526 | ABORT          | Maintenance is currently active on the maximum number of maintenance objects that the system can support. A common cause is that the system contains a large number of administered stations or trunks with installed circuit packs that are not physically connected. Resolve as many alarms as possible on the station and trunk MOs, or busyout these MOs to prevent maintenance activity on them. Then try the command again. |
|                         | NO BOARD       | The circuit pack is not physically installed.                                                                                                                                                                                                                                                                                                                                                                                     |
| 2100                    | EXTRA BD       | This result can appear for Maintenance/Test, Announcement circuit packs MC Call Classifier, Tone Detector, or Speech Synthesis circuit packs. Each of these circuit packs has restrictions on how many can be installed in the system or in a port network, depending on system configuration. Remove any extra circuit packs.                                                                                                    |
| 1                       | FAIL           | For reset commands, the circuit pack was not successfully halted.                                                                                                                                                                                                                                                                                                                                                                 |
| 2                       | FAIL           | For reset commands, the circuit pack was not successfully restarted after being halted. For both results replace the circuit pack.                                                                                                                                                                                                                                                                                                |
|                         | FAIL           | For information about the applicable maintenance object from the <b>Maintenance Name</b> field, see <i>Avaya Aura® Communication Manager Alarms, Events, and Logs Reference</i> .                                                                                                                                                                                                                                                 |
|                         | PASS           | The requested action successfully completed. If the command was a reset, the circuit pack is now running and should be tested.                                                                                                                                                                                                                                                                                                    |

## Auto answer

When you administer **Auto Answer**, the **Communication Manager Endpoint Manager** field displays the following behavior with regards to the **Mute Speakerphone Interaction**, the **Auto Answer** field and the **int aut-an** button:

1. The system does not display the **Turn On Mute for Remote Off-hook Attempt** field for the following configurations:
  - When **Auto Answer** has a value other than **none**.
  - When you enable the **int-aut-an** button for an endpoint.

2. If you enable the **Turn On Mute for Remote Off-hook Attempt** field in the endpoints page, **Communication Manager Endpoint Manager** field does not permit the following administration:
- **Auto Answer** values other than **none**.
  - **int-aut-an** button administration.

## Auto answer field descriptions

In **Expert Agent Environment (EAS)** environment, the auto answer setting for an **Agent LoginID** overrides the endpoint settings when the agent logs in.

| Valid entry | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>  | All ACD and non-ACD calls to an idle station cut through immediately. The agent cannot use automatic hands-free answer for intercom calls. With non-ACD calls, the station rings while the call is cut through. To prevent the station from ringing, activate the ringer-off feature button, provided the <b>Allow Ringer-off with Auto-Answer</b> feature is enabled for the system.                                                                                                    |
| <b>acd</b>  | Only ACD split, ACD skill, and direct agent calls cut through. Non-ACD calls to the station ring tone.<br>For analog stations: <ul style="list-style-type: none"> <li>• Only ACD can perform: <ol style="list-style-type: none"> <li>1. Split calls and Skill calls</li> <li>2. Direct agent calls cut through</li> </ol> </li> <li>• Non-ACD calls receive busy tone. If the station is active on an ACD call and a non-ACD call arrives, the agent hears call-waiting tone.</li> </ul> |
| <b>none</b> | All calls to the station receive a ringing tone.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>icom</b> | The user can answer an intercom call from the same intercom group without pressing the <b>intercom</b> button.                                                                                                                                                                                                                                                                                                                                                                           |

## Turn On Mute for Remote Off-hook Attempt

Using the **Telecommuter** mode of a soft phone or an ASAI, users can control the desk phone remotely. However, users can remotely hear the conversations, which might be considered a privacy breach.

The **Turn On Mute for Remote Off-hook Attempt** field prevents the potential privacy breach in the following manner.

- When users enable the **Turn On Mute for Remote Off-hook Attempt** field on the station screen, any off-hook event on the desk phone turns on the **Mute** button
- When the **Mute** button is active, the user cannot remotely hear conversations

This feature applies to Calls received or originated remotely from soft phones in a shared control mode and Calls received or originated remotely by using ASAI in H.323 configuration. The Communication Manager controls the signaling by activating the mute button for the off-hook event.

## Use case scenario for endpoints set type

### Change Set type of an Endpoint

To change **Set Type** of an **Endpoint**, for example to change from 9630SIP to 9641SIP, do one of the following:

- To change the **Set Type** of an **Endpoint**, default template or custom template of the **Set Type** to be updated can be applied from Endpoint editor, Global Endpoint change or User Management Communication profile section. This operation applies the values of templates in the end point fields and overwrites the values that you entered.
- To change the **Set Type** of an **Endpoint** and keep current data of endpoint such as **COR**, **COS**, **loss group**, do one of the following:
  - **Global Endpoint Change** For more information see Changing endpoint parameters globally.
  - **Element Cut Through** For more information see Element Cut Through.

### Related links

[Use Element Cut Through](#) on page 779

[Changing endpoint parameters globally](#) on page 718

## Configuring the Feature buttons

### Adding a Feature button to the SIP endpoint

#### About this task

Use this procedure to add a Feature button to the SIP endpoint.

#### Before you begin

1. Select a set type of the SIP endpoint that supports the Feature button that you want to add.
2. For the SIP set type that you selected, configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

The system displays the New Endpoint page.

4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. On the **Feature Options** tab:
  - a. Enter the required configuration parameters.
  - b. In the **Features** list, select the features for the SIP endpoint.

6. On the **Button Assignment** tab:
  - a. Click **Feature Buttons**.
  - b. In **Endpoint Configurations**, in the **Button Label** field, type a name for the button. For example, call pick up.
  - c. In **Button Configurations**, in the **Button Feature** field, click the feature button that you want to add. For example, click **call—pkup**.
7. Click **Commit**.

The SIP endpoint displays the **Feature** button that you added.

## Adding the Call Pickup button on an endpoint

### About this task

Use this procedure to specify the number of times that an endpoint must ring for call pick up. For example, System Manager 7.0 supports a Triple Ringer.

### Before you begin

1. Select a set type for your endpoint from the following:
  - 9620
  - 9630
  - 9640
  - 9650
  - 9608
  - 9611
  - 9621
  - 9641
2. For the endpoint set type that you selected, configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. On the **Feature Options** tab:
  - a. Enter the required configuration parameters.
  - b. In the **Features** list, select the features for the SIP endpoint.



6. On the **Button Assignment** tab:
  - a. Click **Feature Buttons**.
  - b. In **Endpoint Configurations**, in the **Button Label** field, type `Call Pickup`.
  - c. In **Button Configurations**, in the **Button Feature** field, click **call-pkup**.
  - d. In the **Rg** field, type the number of times that the endpoint must ring for the call pickup: The options are: `continuous`, `if-busy-silent`, `if-busy-single`, `no-ring`, `single`, `triple`.
7. Click **Commit**.

The endpoint displays the **Call Pickup** button that rings three successive times for call pick up.

## Adding the Service Observe button on a SIP endpoint

### About this task

Use this procedure to add the **Service Observe** button, which is useful in the Contact Center environment for managing and monitoring agent calls. You can add the **Service Observe** button on SIP endpoints in the following modes:

- **listen—only** : To monitor agent calls without interrupting the call
- **so-coach** : To coach an agent during the call

### Before you begin

- Select a set type for your SIP endpoint from the following:
  - 9608SIPCC
  - 9611SIPCC
  - 9621SIPCC
  - 9641SIPCC
- You must configure the endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide* .

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.  
The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. On the **Feature Options** tab:
  - a. Enter the required configuration parameters.
  - b. In the **Features** list, select the features for the SIP endpoint.

6. On the **Button Assignment** tab:
  - a. Click **Feature Buttons**.
  - b. In **Endpoint Configurations**, in the **Button Label** field, type `Service Observe`.
  - c. In **Button Configurations**, in the **Button Feature** field, click **sip-sobsv** mode. The options are:
    - **listen-only**
    - **so-coach**
7. Click **Commit**.

The endpoint displays the **Service Observe** button that you added.

## Adding the VOA Repeat button on a SIP endpoint

### Before you begin

- Select a set type for your SIP endpoint from the following:
  - 9608SIPCC
  - 9611SIPCC
  - 9621SIPCC
  - 9641SIPCC
- Configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide* .

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. On the **Feature Options** tab:
  - a. Enter the required configuration parameters.
  - b. In the **Features** list, select the features for the SIP endpoint.
6. On the **Button Assignment** tab:
  - a. Click **Feature Buttons**.
  - b. In **Endpoint Configurations**, in the **Button Label** field, type `VOA Repeat`.
  - c. In **Button Configurations**, in the **Button Feature** field, click **VOA Repeat**.
7. Click **Commit**.

The endpoint displays the **VOA Repeat** button that you added.

## Adding an Agent skill on a SIP endpoint

### Before you begin

1. Select a set type for your SIP endpoint from the following:
  - 9608SIPCC
  - 9611SIPCC
  - 9621SIPCC
  - 9641SIPCC
2. Configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.  
The system displays the New Endpoint page.
4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. On the **Feature Options** tab:
  - a. Enter the required configuration parameters.
  - b. In the **Features** list, select the features for the SIP endpoint.
6. On the **Button Assignment** tab:
  - a. Click **Feature Buttons**.
  - b. In **Endpoint Configurations**, in the **Button Label** field, type a name for the agent skill.
  - c. In **Button Configurations**, in the **Button Feature** field, click **add-rem-sk**.
7. Click **Commit**.

The SIP endpoint displays the agent skill that you added.

## Creating a Single Administration Dual Registration endpoint

### Before you begin

1. Select a set type for your endpoint from the following:
  - 9608
  - 9610
  - 9611
  - 9620
  - 9621

- 9630
- 9641
- 9650

 **Note:**

The system enables the **Allow H.323 and SIP Endpoint Dual Registration** field only for the set types mentioned in the list.

2. For the endpoint set type that you selected, configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

## Procedure

1. On the System Manager web console, click **Users > User Management**.
2. In the navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, do the following:
  - a. Click **Communication Profile > CM Endpoint Profile**.
  - b. In the **Set Type** field, click the endpoint set type that you want to add.  
For example, click **9608**.
  - c. Select **Allow H.323 and SIP Endpoint Dual Registration** .  
For more information, see *CM Endpoint Profile field descriptions*.
5. Click **Commit**.

## Enabling Reachability on a SIP endpoint

### Before you begin

1. Select a set type for your SIP endpoint from the following:
  - 9608SIP
  - 9611SIP
  - 9621SIP
  - 9641SIP
  - 9608SIPCC
  - 9611SIPCC
  - 9621SIPCC
  - 9641SIPCC
2. Configure the required endpoint template on Communication Manager. For more information, see *Administering Communication Manager Guide*.

## Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. On the Endpoints page, click **New** to add a new endpoint.

The system displays the New Endpoint page.

4. In the **Template** field, click the Communication Manager template that you configured for the set type of your SIP endpoint.
5. In the General Options tab, perform the following:
  - a. In the **Reachability** field, click **System**.
  - b. Select the **Enable Reachability for Domain Control SIP Stations** check box.
6. Click **Commit**.

## Use Element Cut Through

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Manage Endpoints**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Select the Communication Manager endpoint, click **Switch to Classic View > Edit**.
5. On the Element Cut Through page, select **Set Type** to update the template.
6. Click **Enter** to commit the endpoint update.

The updated endpoint is in sync with the System Manager.

---

## Hunt Group

### Hunt Groups

Use the Hunt Groups feature to set up a group of extensions that can handle multiple calls to a single telephone number. You can choose the call distribution method to route calls. For each call to the number, the system hunts for an available extension in the hunt group, and connects the call to that extension.

A hunt group is especially useful when you expect a high number of calls to a particular telephone number. A hunt group might consist of people who are trained to handle calls on specific topics. For example, the group might be a:

- Benefits department within your company
- Service department for products that you sell

- Travel reservations service
- Pool of attendants

A hunt group might also consist of a group of shared telecommunications facilities. For example, the group might be a:

- Modem pool
- Group of data-line circuit ports
- Group of data modules

## Hunt Group List field descriptions

**Hunt Group List** displays all the Hunt Groups that are associated with the selected Communication Manager. You can view the usage list of the extension of the hunt group. You can also apply filters and sort each of the columns in **Hunt Group List**.

When you click **Refresh**, you can view the updated information that is available after the last synchronization operation.

| Name                   | Description                                                       |
|------------------------|-------------------------------------------------------------------|
| <b>Group Number</b>    | The group number of the hunt group.                               |
| <b>Group Name</b>      | The group name of the hunt group.                                 |
| <b>Group Extension</b> | The group extension of the hunt group.                            |
| <b>Group Type</b>      | The group type of the hunt group.                                 |
| <b>Tenant Number</b>   | The tenant number of the hunt group.                              |
| <b>System</b>          | The name of Communication Manager associated with the hunt group. |

## Adding a hunt group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Groups > Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, click **New**.
6. On the New Hunt Group page, in the **General options (O)**, **Message Center Parameters (C)**, and **Group Members (M)** sections, complete the mandatory fields that are marked with a red asterisk (\*).
7. To add the hunt group, click **Commit** or do one of the following:
  - To add the hunt group at the specified time, click **Schedule**. On the Job Scheduler page, set the time, and click **Schedule**.
  - To cancel the operation, click **Cancel**.

## Editing a hunt group

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select the hunt group you want to edit, and do one of the following:
  - Click **Edit**.
  - Click **View** > **Edit**.
6. On the **Edit Hunt Group** page, edit the required fields.
7. Click **Commit** to save the changes.

## Viewing a hunt group

### About this task

Use the following procedure to view the parameters of a hunt group.

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select the hunt group.
6. Click **View**.

On the View Hunt Group page, you cannot edit the fields. To go to the Edit Hunt Group page, click **Edit**.

## Deleting a hunt group

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Groups** > **Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.

5. In the **Hunt Group List** section, select a hunt group, and click **Delete**.
6. On the Delete Hunt Group Confirmation page, do one of the following:
  - To delete the hunt group immediately, click **Delete**.
  - To delete the hunt group at the specified time, click **Schedule**. On the Job Scheduler page, set the time, and click **Schedule**.
  - To cancel the operation, click **Cancel**.

## List Usage Extension in hunt group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Groups > Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Hunt Group List** section, select a hunt group.
6. Click **More Actions > List Usage Extension**.

The system displays the **List Usage Extension** page with details.
7. Click **Done**.

## Exporting selected hunt group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Groups > Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the **Hunt Group List**, select the hunt group you want to export.
6. Click **More Actions > Export Selected Hunt Group**.

The system displays the **Export Hunt Group** page.
7. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
8. Click **Export**.

## Exporting all hunt groups

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Groups > Hunt Group**.



3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Export All Hunt Groups**.  
The system displays the **Export Hunt Group** page.
6. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
7. Click **Export**.

## Importing hunt groups

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Groups > Hunt Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Import Hunt Groups**.  
The system displays the **Import CM Objects** page.
6. In the **Select a file** field, select the required excel file and click **Browse**.
7. Select one of the following in the **Select Error Configuration** field.  
Default value is **Continue processing other records**.
  - **Abort on first error**
  - **Continue processing other records**
8. Select one of the following in the **If a matching record already exists** field.  
Default value is **Skip**.
  - **Skip**
  - **Merge**
  - **Delete**
9. In the **Schedule Job** field, click **Run immediately** or **Schedule later**.
10. Click **Import**.

## Downloading Excel Template

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Groups > Hunt Group**.

3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **More Actions > Download Excel Template**.
6. In the **Opening <Excel template file name>.xlsx** dialog box, click **Save**, and click **OK**.

---

## Trunk Group

### Trunk Group List field descriptions

**Trunk Group List** displays all the Trunk Groups that are associated with the selected Communication Manager. You can also apply filters and sort each of the columns in **Trunk Group List**.

When you click **Refresh**, you can view the updated information that is available after the last synchronization operation.

| Name                     | Description                                        |
|--------------------------|----------------------------------------------------|
| <b>Group Number</b>      | The group number of the trunk group.               |
| <b>Trunk Group Name</b>  | The group name of the trunk group.                 |
| <b>Group Type</b>        | The group type of the trunk group.                 |
| <b>Tenant Number</b>     | The tenant number of the trunk group.              |
| <b>TAC</b>               | The trunk access code (TAC) of the trunk group.    |
| <b>Number of Members</b> | The number of members of the trunk group.          |
| <b>COR</b>               | The class of restriction (COR) of the trunk group. |
| <b>CDR</b>               | The call detail record (CDR) of the trunk group.   |
| <b>Outgoing Display</b>  | The outgoing display of the trunk group.           |
| <b>Queue Length</b>      | The queue length of the trunk group.               |
| <b>System</b>            | The system of the trunk group.                     |

### Adding a trunk group

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Network > Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, click **New**.

6. On the New Trunk Group page, complete the mandatory fields that are marked with a red asterisk (\*) in the following sections:
  - General Options (O)
  - Parameter Options (P)
  - Feature Options (F)
  - Administrable Timer (A)
  - ATM Thresholds (T)
  - Group Members (M)
7. Click one of the following:
  - **Commit**: To add the trunk group.
  - **Schedule**: To add the trunk group at a specific time. On the Job Scheduler page, set the time, and click **Schedule**.
  - **Cancel**: To cancel the operation.

## Editing a trunk group

### About this task

You can edit one trunk group at a time. If you select more than one trunk group the system disables the **View** and **Edit** options.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Network > Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, select the trunk group that you want to edit, and click **Edit**.
6. On the **Edit Trunk Group** page, edit the required fields.
7. Click **Commit** to save the changes.

## Viewing a trunk group

### About this task

Use this procedure to view the parameters of a trunk group. If you select more than one trunk group the system disables the **View** and **Edit** options.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.

2. In the left navigation pane, click **Network > Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, select the trunk group.
6. Click **View**.

The system displays the View Trunk Group page.

## Deleting a trunk group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Network > Trunk Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. In the **Trunk Group List** section, select one or more trunk groups, and click **Delete**.
6. On the Delete Trunk Group Confirmation page, click one of the following:
  - **Delete**: To delete the Trunk group immediately.
  - **Schedule**: To delete the Trunk group at the specified time. On the Job Scheduler page, set the time, and click **Schedule**.
  - **Cancel**: To cancel the operation.

---

## Managing Off PBX Configuration Set

### Viewing Off PBX Configuration Set

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Off PBX Telephone > Off PBX Configuration Set**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Off PBX Configuration Set list, select the Off PBX Configuration Set you want to view.
6. Click **View**.

You can view the details of the Off PBX Configuration Set through the classic view.

## Editing Off PBX Configuration Set

### Procedure

1. On the System Manager web console, click **Elements** > **Communication Manager**.
2. In the navigation pane, click **Endpoints** > **Off PBX Telephone** > **Off PBX Configuration Set**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Off PBX Configuration Set list, select the Off PBX Configuration Set you want to edit.
6. Click **Edit**.

You can edit the Off PBX Configuration Set details through the classic view.

7. To save the changes, click **Enter**.

## Off PBX Configuration Set field descriptions

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Number</b>               | The Off PBX endpoint configuration set number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>          | Description of the Off PBX endpoint configuration set. The description field can also specify the name of the Off PBX Configuration Set.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Calling Number Style</b> | <p>Determines the format of the caller ID for calls from a local Communication Manager extension to an extension to a cellular telephone. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Network:</b> Provides a display of only 10-digit numbers. For internal calls, the ISDN numbering tables are used to create the calling number. DCS calls use the ISDN calling number, if provided. Externally provided calling numbers are used for externally originated calls.</li> <li>• <b>Port:</b> Provides a display of less than 10-digits. Extensions are sent as the calling number for all internal and DCS network-originated calls.</li> </ul> |

*Table continues...*

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CDR Origination</b> | <p>Determines the Call Detail Record (CDR) report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone. To generate this CDR, you must enable the Incoming Trunk CDR. The CDR report excludes dialed Feature Name Extensions (FNEs). The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>phone-number</b>: The calling party on the CDR report is the 10-digit cell phone number. This is the default value.</li> <li>• <b>extension</b>: The calling party on the CDR report is the internal office telephone extension associated with the Extension to Cellular cell phone.</li> <li>• <b>none</b>: The system does not generate an originating CDR report.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>CDR EC500</b>       | <p>Determines whether a CDR is generated for any call to the cellular telephone. Available only if CDR reports are enabled for the trunk group. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>true</b>: Treats calls to the XMOBILE station as trunk calls and generates a CDR.</li> <li>• <b>false</b>: Treats calls to the XMOBILE station as internal calls, without generating a CDR.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Fast Conn</b>       | <p>Determines whether additional processing occurs on the server running Communication Manager prior to connecting a call. Fast Conn is reserved for future that the cell telephone provider might provide.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Post Conn</b>       | <p>Determines whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped to XMOBILE endpoints. Post Conn options come into effect after the call has entered the active state. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>dtmf</b>: Expect digits from either in-band or out-of-band, but not simultaneously. The server allocates a DTMF receiver whenever the server needs to collect digits. This option is normally used for Extension to Cellular XMOBILE endpoint calls.</li> <li>• <b>out-of-band</b>: Expect all digits delivered by out-of-band signaling only. The server running Communication Manager collects digits from the out-of-band channel or no touch-tone receiver. In addition, any digits received when the server is not collecting digits are converted to DTMF and is broadcast to all the parties on the call. This option is implemented for DECT XMOBILE endpoint calls.</li> <li>• <b>both</b>: Expect all subsequent digits delivered by simultaneous in-band and out of-band signaling. Out-of-band signaling consists of digits embedded in ISDN INFO messages while in-band signaling consists of DTMF in the voice path. The server running Communication Manager collects all the digits from the out-of-band channel. To prevent double digit collection, touch tone receive is not allocated. End-to-end signaling occurs transparently to the server through in-band transmission of DTMF. This option is implemented for PHS XMOBILE endpoint calls.</li> </ul> |

*Table continues...*

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Voice Mail Dest</b> | <p>Voice Mail Dest prevents cellular voice mail from answering an Extension to Cellular call. When the call server detects that the cell phone is not the entity answering the call, the call server brings the call back to the server. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>none</b>: No restrictions on cellular voice mail. This is the default value.</li> <li>• <b>timed</b>: When you enter timed, the system displays the seconds field, which accepts values from 1 to 9. The default value is 4 seconds. In the Extension to Cellular-enabled environment, if you answer the call at the cell within the configured time, Communication Manager treats the call as a call that the cellular voice mail answers, and disconnects the cellular leg of the call. The call continues to ring at the desk phone. You can use this configuration for any type of network, including GSM, CDMA, and ISDN.</li> <li>• <b>message</b>: The message option works with carriers who use non-ISDN voice mail systems. You must not use this option with ISDN-based voice mail systems.</li> </ul> |
| <b>System</b>          | The name of the Communication Manager system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Button      | Description                                                 |
|-------------|-------------------------------------------------------------|
| <b>View</b> | Click to view the details of the Off PBX Configuration Set. |
| <b>Edit</b> | Click to edit the Off PBX Configuration Set.                |

## Managing Off PBX Endpoint Mapping

### Adding Off PBX Endpoint Mapping to an endpoint

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Off PBX Telephone > Off PBX Endpoint Mapping**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Add Off PBX Endpoint Mapping through the SAT screen.
7. Click **Enter**.

## Viewing the Off PBX Endpoint Mapping

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Off PBX Telephone > Off PBX Endpoint Mapping**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Off PBX Endpoint Mapping that you want to view.
6. Click **View**.

The system displays the details of the Off PBX Endpoint Mapping from the classic view.

## Editing the Off PBX Endpoint Mapping of an endpoint

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Off PBX Telephone > Off PBX Endpoint Mapping**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Off PBX Endpoint Mapping you want to edit.
6. Click **Edit**.
7. Edit the required fields through the SAT screen.
8. To save the changes, click **Enter**.

## Off PBX Endpoint Mapping field descriptions

| Name                      | Description                                                                                                                                                                                                                                                                                                             |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Endpoint Extension</b> | The SIP and non-SIP extensions that have Off PBX Endpoint Mapping.<br><br>When you add a SIP endpoint, an entry for this endpoint is automatically available in Off PBX Endpoint Mapping.<br><br>To add an endpoint mapping to a non-SIP endpoint, you must manually add an Off PBX Endpoint Mapping for that endpoint. |
| <b>System</b>             | The Communication Manager system in which the endpoint extension is available.                                                                                                                                                                                                                                          |



| Button      | Description                                  |
|-------------|----------------------------------------------|
| <b>New</b>  | Adds an Off PBX Endpoint mapping.            |
| <b>View</b> | Displays an Off PBX mapping for an endpoint. |
| <b>Edit</b> | Edits an Off PBX Endpoint mapping.           |

## Xmobile Configuration

### Xmobile Configuration

Xmobile Configuration defines the number of call treatment options for Extension to Cellular calls for cellular telephones. The Extension to Cellular feature allows the use of up to 99 Configuration Sets, already defined in the system using default values.

### Xmobile Configuration List

Xmobile Configuration List displays the Xmobile Configuration details under the Communication Manager you select. You can apply filters and sort each column in this list.

Click **Refresh** to view the updated information after the last synchronization.

| Name                        | Description                                                                                                                                                      |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configuration Set</b>    | The configuration set value.                                                                                                                                     |
| <b>Calling No.</b>          | The format of the caller ID for calls from a local switch extension to an EC500 cell phone.                                                                      |
| <b>CDR Orig</b>             | The CDR report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone.                                        |
| <b>CDR EC 500</b>           | Displays whether a call detail record is generated for any call to the cell phone.                                                                               |
| <b>Fast Conn</b>            | Displays whether some additional processing occurs on the switch prior to connecting a call.                                                                     |
| <b>Post-Connect Dialing</b> | Displays whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped into XMOBILE stations. |
| <b>System</b>               | The name of the Communication Manager associated with the Xmobile Configuration set.                                                                             |

## Viewing Xmobile Configuration data

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Xmobile Configuration**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. From the Xmobile Configuration List, select the configuration set you want to view.
6. Click **View**.

#### Related links

[Xmobile Configuration field descriptions](#) on page 792

## Editing Xmobile Configuration

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Endpoints > Xmobile Configuration**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Xmobile Configuration List, select the configuration set you want to view.
6. Click **Edit** or click **View > Edit**.
7. Edit the required details on the **Edit Xmobile Configuration Data** page.
8. Click **Commit** to save the changes.

#### Related links

[Xmobile Configuration field descriptions](#) on page 792

## Xmobile Configuration field descriptions

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Barge-in Tone</b>        | Enables a barge-in tone used to add security to Extension to Cellular calls. If a user is on an active Extension to Cellular call and another person joins the call from an Extension to Cellular enabled office telephone, all parties on the call hear the barge-in tone.                                                                                                                                                                                                                                                                                                                                                            |
| <b>Calling Number Style</b> | <p>Determines the format of the caller ID for calls from a local switch extension to an EC500 cell phone.</p> <ul style="list-style-type: none"> <li>• <b>network</b>: Provides a display of only 10-digit numbers. For internal calls, the ISDN numbering tables are used to create the calling number and DCS calls use the ISDN calling number if provided. The externally provided calling number is used when available for externally originated calls.</li> <li>• <b>pbx</b>: Provides a display of less than 10-digits. Extensions sent as the calling number for all internally- and DCS network-originated calls.</li> </ul> |

*Table continues...*

| Name                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CDR for Calls to EC500 Destination</b> | <p>Determines whether a call detail record is generated for calls to the cell phone.</p> <p> <b>Note:</b></p> <p>CDR reporting for EC500 calls relies on the CDR Reports field on the Trunk Group screen. If, on the Trunk Group screen, the CDR Reports field is set to <b>n</b>, no CDR is generated even if this field is set to <b>y</b>.</p> <ul style="list-style-type: none"> <li>• <b>y</b>: Treats calls to the XMOBILE station as trunk calls and generates a CDR.</li> <li>• <b>n</b>: Treats calls to the XMOBILE station as internal calls and does not generate a CDR.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Configuration Set Description</b>      | Describes the purpose of the configuration set. A valid entry is up to 20 alphanumeric characters or blank. For example, EC500 handsets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Fast Connect on Origination</b>        | Determines whether some additional processing occurs on the switch prior to connecting a call. You can use the <b>y</b> option to send CONNECT messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Post-Conn Signaling</b>                | <p>Post Connect Dialing Options. Determines whether additional capabilities, beyond standard ISDN dialing, are available for those incoming ISDN trunk calls that are mapped into XMOBILE stations. These options come into effect after the call has entered the active state when the switch has sent a CONNECT message back to the network.</p> <ul style="list-style-type: none"> <li>• <b>dtmf</b>: Expect digits from either in-band or out-of-band, but not simultaneously. The switch allocates a DTMF receiver whenever it needs to collect digits. This option is generally used for EC500 XMOBILE station calls.</li> <li>• <b>out-of-band</b>: Expect all digits to be delivered by out-of-band signaling only. The switch collects digits that it needs from the out-of-band channel (no touch-tone receiver). In addition, any digits received when the switch is not collecting digits are converted to DTMF and broadcast to all parties on the call. This option is in force for DECT XMOBILE station calls.</li> <li>• <b>both</b>: Expect all subsequent digits to be delivered by simultaneous in-band and out-of-band signaling. Out-of-band signaling consists of digits embedded in ISDN INFO messages while the in-band signaling consists of DTMF in the voice path. The switch collects all digits that it needs from the out-of-band channel. No touch tone receive is allocated in order to prevent collecting double digits. End-to-end signaling occurs transparently to the switch through in-band transmission of DTMF. This option is in force for PHS XMOBILE station calls.</li> </ul> |

*Table continues...*

| Name                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Call Appearance Selection for Origination</b> | <p>Specifies how the system selects a Call Appearance for call origination. To use this feature, bridged calls must be enabled for the system.</p> <ul style="list-style-type: none"> <li>• <b>first-available:</b> The system searches for the first available regular or bridged Call Appearance.</li> <li>• <b>primary-first:</b> Only regular Call Appearances are used for call origination. If a regular call appearance is not available, the call is not allowed. The system first searches for a regular Call Appearance for call origination. If a regular Call Appearance is not available, a second search is made that includes both regular and bridged Call Appearances. This is the default setting.</li> </ul> |
| <b>Calling Number Verification</b>               | <p>Enables restrictions on the types of calls made to a cell phone with Extension to Cellular.</p> <ul style="list-style-type: none"> <li>• <b>y:</b> Prevents all calls, except for the following calls, from reaching the cell phone: <ul style="list-style-type: none"> <li>- Network-provided</li> <li>- User-provided</li> <li>- Passed</li> </ul> <p>This setting has no effect on normal usage of the Extension to Cellular feature. This is the default setting.</p> </li> <li>• <b>n:</b> No restrictions on calls to the cell phone.</li> </ul>                                                                                                                                                                       |
| <b>CDR for Origination</b>                       | <p>Determines the CDR report format when CDR records are generated for a call that originates from an Extension to Cellular cell phone. To generate this CDR, you must enable the Incoming Trunk CDR. The CDR report does not include dialed Feature Name Extensions (FNEs).</p> <ul style="list-style-type: none"> <li>• <b>phone-number:</b> The calling party on the CDR report is the 10-digit cell phone number. This is the default setting.</li> <li>• <b>extension:</b> The calling party on the CDR report is the internal office telephone phone extension associated with the Extension to Cellular cell phone.</li> <li>• <b>none:</b> The system does not generate an originating CDR report.</li> </ul>           |

*Table continues...*

| Name                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cellular Voice Mail Detection</b> | <p>Prevents cellular voice mail from answering an Extension to Cellular call. The call server detects when the cell phone is not the entity that answers the call and brings the call back to the server. Communication Manager treats the call as a normal call to the office telephone and the call goes to corporate voice mail. You can also set a timer for cellular voice mail detection that sets a time before Cellular Voice Mail Detection investigates a call.</p> <ul style="list-style-type: none"> <li>• <b>none:</b> No restrictions on cellular voice mail. This is the default setting.</li> <li>• <b>timed:</b> Amount of time from 1 to 9 seconds. The default time is 4 seconds. Extension to Cellular call leg answered within the specified time is detected as being answered by the cellular voice mail and the call continues to ring at the office telephone. If unanswered, it will go to the corporate voice mail. This setting can be used for different types of network that is, GSM, CDMA, and ISDN.</li> <li>• <b>message:</b> The message option works with carriers who use non ISDN voice mail systems. Avoid using this option with ISDN-based voice mail systems.</li> </ul> |
| <b>Confirmed Answer</b>              | <p>Enables Confirmed Answer on Extension to Cellular calls for this station. If you select this option, the user needs to input a digit to confirm receipt of a call sent to a cell phone using the Extension to Cellular feature. When the user answers the incoming call on the cell phone, the user hears a dial tone. The user must then press any one of the digits on the cell phone keypad. Until the system receives a digit, the system does not treat the call as answered. The length of time to wait for the digit can be administered from 5 to 20 seconds, with a default of 10 seconds. The system plays a recall dial tone to indicate that input is expected. During the response interval, the original call continues to alert at the desk phone and any stations bridged to the call. If the user does not enter a digit before the time-out interval expires, the call is pulled back from the telephone device.</p>                                                                                                                                                                                                                                                                          |
| <b>Configuration Set ID</b>          | The configuration set value that you selected in the Xmobile Configuration List. This is a display-only field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Completes the action you initiate.                                  |
| <b>Schedule</b> | Performs the action at the chosen time.                             |
| <b>Reset</b>    | Clears the action and resets the field.                             |
| <b>Clear</b>    | Clears all the entries.                                             |
| <b>Edit</b>     | Allows you to edit the fields in the page.                          |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>      | Performs the action you initiate real time.                         |

---

## Automatic Alternate Routing Digit Conversion

### AAR/ARS Digit Conversion

Use the Automatic Alternate Routing (AAR) Digit Conversion or Automatic Route Selection (ARS) Digit Conversion capability to configure your system to change a dialed number for efficient routing by inserting or deleting digits from the dialed number. For instance, you can configure the server running Communication Manager to delete **1** and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

### Viewing Automatic Alternate Routing Digit Conversion data

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Automatic Alternate Routing Digit Conversion**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the AAR Digit Conversion List, select the Automatic Alternate Routing Digit Conversion data you want to view.
6. Click **View**.

#### Related links

[AAR/ARS Digit Conversion field descriptions](#) on page 797

### Editing Automatic Alternate Routing Digit Conversion data

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Automatic Alternate Routing Digit Conversion**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the AAR Digit Conversion List, select the Automatic Alternate Routing Digit Conversion you want to edit.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit AAR Digit Conversion** page.
8. Click **Commit** to save the changes.

#### Related links

[AAR/ARS Digit Conversion field descriptions](#) on page 797

## AAR/ARS Digit Conversion field descriptions

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ANI Required</b>     | <p>This field applies only if the Request Incoming ANI (non-AAR/ARS) field on the Multifrequency-Signaling-Related System Parameters screen is set to <b>n</b>.</p> <ul style="list-style-type: none"> <li>• <b>y</b> or <b>n</b>: Enter <b>y</b> to require ANI on incoming R2-MFC or Russian MF ANI calls. The entry must be set to <b>y</b> to enable EC500 origination features.</li> <li>• <b>r</b>: Restricted. Allowed only if the Allow ANI Restriction on AAR/ARS field is set to <b>y</b> on the Feature-Related System Parameters screen. Use this entry to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat <b>r</b> as <b>y</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Conv</b>             | Provides the option to allow additional digit conversion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Del</b>              | The number of digits you want the system to delete from the beginning of the dialed string. A valid entry ranges from <b>0</b> to <b>Min</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Location</b>         | <p>This is a display-only field. Typing the command <code>change aar digit-conversion n</code> or <code>change ars digit-conversion n</code> displays the all-locations screen, and populates this field with <b>all</b>. The <b>n</b> specifies that dialed strings beginning with the value <b>n</b> are displayed first. To access a per-location screen, type <code>change aar digit-conversion location n</code> or <code>change ars digit-conversion location n</code>, where <b>n</b> represents the number of a specific location. This field then displays the number of the specified location. For details on command options, see online help, or <i>Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers</i>, 03-300431.</p> <p>One of the following is a valid entry:</p> <ul style="list-style-type: none"> <li>• <b>1</b> to <b>64</b>: Specifies whether you require ANI on incoming R2-MFC or Russian MF ANI calls. Entry must be <b>y</b> to enable EC500 origination features.</li> <li>• <b>all</b>: Indicates that this AAR/ARS Digit Conversion Table is the default for all port network (cabinet) locations.</li> </ul> |
| <b>Matching Pattern</b> | Specifies the number you want the server running Communication Manager to match to dialed numbers. If a prefix digit <b>1</b> is required for 10-digit direct distance dialing (DDD) numbers, be sure the matching pattern begins with a 1. A valid entry is a number ranging from <b>0</b> to <b>9</b> (1 to 18 digits) and wildcard characters asterisk (*), <b>x</b> , and <b>X</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Max</b>              | The maximum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from <b>Min</b> to <b>28</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Min</b>              | The minimum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from <b>1</b> to <b>Max</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Net</b>              | The call-processing server network used to analyze the converted number. The entries <b>ext</b> , <b>aar</b> , or <b>ars</b> analyze the converted digit-string as an extension number, an AAR address, or an ARS address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Percent Full</b>       | Displays the percentage from <b>0</b> to <b>100</b> of the system memory resources that have been used by ARS. If the figure is close to 100 percent, you can free-up memory resources.                                                                                                                                                                                                                |
| <b>Replacement String</b> | A valid entry ranges from <b>0</b> to <b>9</b> (1 to 18 digits), asterisk (*), pound (#), or blank. Enter the digits that replace the deleted portion of the dialed number.<br><br>If the pound character (#) is present in the string, it should be the last character in the string. This signifies the end of the modified digit string.<br><br>Leave this field blank to simply delete the digits. |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Completes the action you initiate.                                  |
| <b>Schedule</b> | Performs the action at the chosen time.                             |
| <b>Reset</b>    | Clears the action and resets the field.                             |
| <b>Clear</b>    | Clears all the entries.                                             |
| <b>Edit</b>     | Allows you to edit the fields in the page.                          |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>      | Performs the action you initiate real time.                         |

## Automatic Route Selection Digit Conversion

### AAR/ARS Digit Conversion

Use the Automatic Alternate Routing (AAR) Digit Conversion or Automatic Route Selection (ARS) Digit Conversion capability to configure your system to change a dialed number for efficient routing by inserting or deleting digits from the dialed number. For instance, you can configure the server running Communication Manager to delete **1** and an area code on calls to one of your locations, and avoid long-distance charges by routing the call over your private network.

### Viewing Automatic Route Selection Digit Conversion data

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Automatic Route Selection Digit Conversion**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the ARS Digit Conversion List, select the Automatic Route Selection Digit Conversion you want to view.



6. Click **View**.

#### Related links

[AAR/ARS Digit Conversion field descriptions](#) on page 797

## Editing Automatic Route Selection Digit Conversion data

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Automatic Route Selection Digit Conversion**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Edit** or click **View > Edit**.
6. Edit the required fields on the **Edit ARS Digit Conversion** page.
7. Click **Commit** to save the changes.

#### Related links

[AAR/ARS Digit Conversion field descriptions](#) on page 797

## AAR/ARS Digit Conversion field descriptions

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ANI Required</b> | <p>This field applies only if the Request Incoming ANI (non-AAR/ARS) field on the Multifrequency-Signaling-Related System Parameters screen is set to <b>n</b>.</p> <ul style="list-style-type: none"> <li>• <b>y</b> or <b>n</b>: Enter <b>y</b> to require ANI on incoming R2-MFC or Russian MF ANI calls. The entry must be set to <b>y</b> to enable EC500 origination features.</li> <li>• <b>r</b>: Restricted. Allowed only if the Allow ANI Restriction on AAR/ARS field is set to <b>y</b> on the Feature-Related System Parameters screen. Use this entry to drop a call on a Russian Shuttle trunk or Russian Rotary trunk if the ANI request fails. Other types of trunks treat <b>r</b> as <b>y</b>.</li> </ul> |
| <b>Conv</b>         | Provides the option to allow additional digit conversion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Del</b>          | The number of digits you want the system to delete from the beginning of the dialed string. A valid entry ranges from <b>0</b> to <b>Min</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Location</b>           | <p>This is a display-only field. Typing the command <code>change aar digit-conversion n</code> or <code>change ars digit-conversion n</code> displays the all-locations screen, and populates this field with <b>all</b>. The <i>n</i> specifies that dialed strings beginning with the value <i>n</i> are displayed first. To access a per-location screen, type <code>change aar digit-conversion location n</code> or <code>change ars digit-conversion location n</code>, where <i>n</i> represents the number of a specific location. This field then displays the number of the specified location. For details on command options, see online help, or <i>Maintenance Commands for Avaya Aura™ Communication Manager, Media Gateways and Servers</i>, 03-300431.</p> <p>One of the following is a valid entry:</p> <ul style="list-style-type: none"> <li>• <b>1 to 64</b>: Specifies whether you require ANI on incoming R2-MFC or Russian MF ANI calls. Entry must be <code>y</code> to enable EC500 origination features.</li> <li>• <b>all</b>: Indicates that this AAR/ARS Digit Conversion Table is the default for all port network (cabinet) locations.</li> </ul> |
| <b>Matching Pattern</b>   | Specifies the number you want the server running Communication Manager to match to dialed numbers. If a prefix digit <b>1</b> is required for 10-digit direct distance dialing (DDD) numbers, be sure the matching pattern begins with a 1. A valid entry is a number ranging from <b>0</b> to <b>9</b> (1 to 18 digits) and wildcard characters asterisk (*), <b>x</b> , and <b>X</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Max</b>                | The maximum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from <b>Min</b> to <b>28</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Min</b>                | The minimum number of user-dialed digits the system collects to match to this Matching Pattern. A valid entry ranges from <b>1</b> to <b>Max</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Net</b>                | The call-processing server network used to analyze the converted number. The entries <b>ext</b> , <b>aar</b> , or <b>ars</b> analyze the converted digit-string as an extension number, an AAR address, or an ARS address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Percent Full</b>       | Displays the percentage from <b>0</b> to <b>100</b> of the system memory resources that have been used by ARS. If the figure is close to 100 percent, you can free-up memory resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Replacement String</b> | <p>A valid entry ranges from <b>0</b> to <b>9</b> (1 to 18 digits), asterisk (*), pound (#), or blank. Enter the digits that replace the deleted portion of the dialed number.</p> <p>If the pound character (#) is present in the string, it should be the last character in the string. This signifies the end of the modified digit string.</p> <p>Leave this field blank to simply delete the digits.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Button          | Description                             |
|-----------------|-----------------------------------------|
| <b>Commit</b>   | Completes the action you initiate.      |
| <b>Schedule</b> | Performs the action at the chosen time. |
| <b>Reset</b>    | Clears the action and resets the field. |

Table continues...

| Button        | Description                                                         |
|---------------|---------------------------------------------------------------------|
| <b>Clear</b>  | Clears all the entries.                                             |
| <b>Edit</b>   | Allows you to edit the fields in the page.                          |
| <b>Done</b>   | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b> | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>    | Performs the action you initiate real time.                         |

## Automatic Route Selection Toll

### Automatic Route Selection Toll

With Automatic Route Selection Toll, you can specify whether calls to CO codes listed on the table are toll or non-toll calls. You can specify non-toll calls based on the last two digits of the distant-end of the trunk group.

### Automatic Route Selection Toll List

| Name                                    | Description                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>ARS Toll Table</b>                   | The Automatic Route Selection Toll table number.                                                |
| <b>From Office Code, To Office Code</b> | The block of numbers for the associated Automatic Route Selection Toll table.                   |
| <b>System</b>                           | The name of the Communication Manager associated with the Automatic Route Selection Toll table. |

## Viewing Automatic Route Selection Toll data

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Automatic Route Selection Toll**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Automatic Route Selection Toll List, select the Ars Toll Table you want to view.
6. Click **View**.

### Related links

[Automatic Route Selection Toll field descriptions](#) on page 802

## Editing Automatic Route Selection Toll data

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.

2. In the navigation pane, click **Network > Automatic Route Selection Toll**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Automatic Route Selection Toll List, select the Ars Toll Table you want to edit.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit Automatic Route Selection Toll** page.
8. Click **Commit** to save the changes.

#### Related links

[Automatic Route Selection Toll field descriptions](#) on page 802

### Automatic Route Selection Toll field descriptions

| Name                          | Description                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>00:</b> through <b>99:</b> | The last two digits of the codes within the 100-block of numbers. Designate each as a number toll or non-toll call. |
| <b>Ars Toll Table</b>         | The number of the ARS Toll table. Valid entry ranges from <b>2</b> through <b>9</b> .                               |
| <b>Office Codes</b>           | The block of numbers. Valid entry ranges from <b>200</b> to <b>299</b> through <b>900</b> to <b>999</b> .           |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Performs the action you initiate.                                   |
| <b>Schedule</b> | Performs the action at the specified time.                          |
| <b>Reset</b>    | Clears the action and resets the fields.                            |
| <b>Clear</b>    | Clears all entries.                                                 |
| <b>Done</b>     | Completes your current action and navigates to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and navigates to the previous page.     |
| <b>Backup</b>   | Backs up the audio files that you select.                           |
| <b>Now</b>      | Performs the action you initiate real time.                         |

---

## Cluster Session Manager

### Cluster Session Manager

Using the Cluster Session Manager, you can administer a list of unique node names having Session Manager IPs that are configured on Communication Manager. This eliminates the need for provisioning trunks for redundancy. This feature frees up trunks so that the available trunks can be used by SIP agents, SIP stations, or PSTN bound SIP trunk calls. You can also generate reports for displaying the status of active and idle trunks.

With Cluster Session Manager, you can manage up to 10 clusters, and each cluster can manage up to 28 Session Managers. From the Manage Users page, you can define the Primary Session Manager and the Secondary Session Manager. If the call to the SIP station is routed to a SIP trunk that has a clustered signaling group, then the Invite is sent to the station on primary Session Manager. If the primary Session Manager is not reachable, then the Invite is sent to the station on secondary Session Manager.

Using the Signaling Groups page, you can access the Communication Manager CLI and administer the Clustered and Cluster ID fields. These fields appear for SIP signaling groups only. For more information, see “Cluster Session Manager” chapter in *Avaya Aura® Communication Manager Screen Reference* and “SIP trunk optimization” chapter in *Avaya Aura® Communication Manager Feature Description and Implementation*.

## Limitations

Limitations of Cluster Session Manager are as follows:

- You can configure Session Manager node names with IPv6 addresses, only if “procr6” is configured on Communication Manager
- You can configure Session Manager node names with IPv4 addresses, only if “procr” is configured on Communication Manager
- You cannot configure the same node names of type IPv4 and IPv6 in the same cluster

## Viewing cluster Session Managers

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Cluster Session Manager**
3. Click **Show List**.
4. From the Cluster List, select the cluster you want to view.
5. Click **View**.

## Editing cluster Session Managers

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Cluster Session Manager**
3. Click **Show List**.
4. From the Cluster List, select the cluster you want to edit.
5. Click **Edit** or click **View > Edit**.
6. Edit the required fields on the **Edit Cluster** page.
7. Click **Commit** to save the changes.

---

## Data Modules

### Data Modules

Use this capability to connect systems running Communication Manager with other communications equipment, changing protocol, connections, and timing as necessary. Communication Manager supports the following types of data modules:

- High speed links
- Data stands
- Modular-processor data module
- 7000-series data modules
- Modular-trunk data module
- Asynchronous Data Unit
- Asynchronous Data Module for ISDN-Basic Rate Interface telephones
- Terminal adapters

All of these data modules support industry standards and include options for setting the operating profile to match that of the data equipment.

### Data Module List

Data Module List displays all the data modules under the Communication Manager you select. You can apply filters and sort each column in the Data Module List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name             | Description                                                                        |
|------------------|------------------------------------------------------------------------------------|
| <b>Extension</b> | The extension assigned to the data module.                                         |
| <b>Port</b>      | The port location to which the selected data module is connected.                  |
| <b>Type</b>      | The type of data module.                                                           |
| <b>Name</b>      | The name of the user associated with the data module.                              |
| <b>COS</b>       | The desired Class Of Service.                                                      |
| <b>COR</b>       | The desired Class Of Restriction.                                                  |
| <b>TN</b>        | The tenant number which determines the music source for callers on hold.           |
| <b>ISN</b>       | Information Systems Network. Used with Data Line and Processor/Trunk Data Modules. |
| <b>System</b>    | The name of the Communication Manager associated with the data module.             |

## Adding a Data Module

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Data Modules**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select **New**.
6. Complete the **Add Data Module** page and click **Commit**.

### Related links

[Data Modules field descriptions](#) on page 806

## Viewing a Data Module

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Data Modules**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data module you want to view.
6. Click **View**.

### Related links

[Data Modules field descriptions](#) on page 806

## Editing a Data Module

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Data Modules**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data module you want to edit.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit Data Modules** page.
8. Click **Commit** to save the changes.

**Related links**

[Data Modules field descriptions](#) on page 806

**Deleting Data Modules****Procedure**

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Network > Data Modules**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Data Modules List, select the data modules you want to delete.
6. Click **Delete**.
7. Confirm to delete the data modules.

**Related links**

[Data Modules field descriptions](#) on page 806

**Data Modules field descriptions**

| Name                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>List Type</b>                                       | Indicates whether the type of list is group, personal, enhanced, or system type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Special Dialing Option</b>                          | Identifies the destination of all calls when this data module originates calls. The available dialing options are: <ul style="list-style-type: none"> <li>• <b>hot-line</b>: Allows single-line telephone users to automatically place a call to an extension, telephone number, or Feature Access Code (FAC).</li> <li>• <b>default</b>: An associated Abbreviated Dialing number is dialed when the user goes off-hook and enters a carriage return following the DIAL prompt.</li> </ul>                                                                                                                              |
| <b>Personal/Group Number</b>                           | The identifying number the server running Communication Manager assigns to the group when it is created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Abbreviated Dialing Dial Code (From above list)</b> | Used with 7500, Data Line, Netcon, Processor/Trunk, Processor Interface, and World Class BRI Data Modules. System displays this field only when the Special Dialing Option field is default. When the user goes off-hook and enters a carriage return following the DIAL prompt, the system dials the abbreviated dialing number. The data call originator can also perform data-terminal dialing by specifying a dial string that may or may not contain alphanumeric names.<br><br>Valid entry ranges from <b>0</b> through <b>999</b> . You need to enter a list number associated with the abbreviated dialing list. |

*Table continues...*



| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>BCC</b>                    | <p>Bearer Capability Class. A display-only field used with Data Line, Netcon, Processor Interface, Point-to-Point Protocol, Processor/Trunk (pdm selection), and System Port Data Modules. Appears when the <b>ISDN-PRI or ISDN-BRI Trunks</b> field is set to <i>y</i> on the System Parameters Customer-Options (Optional Features) screen. The value in this field corresponds to the speed setting of the data module. This field can be compared with the Bearer Capability Classes (BCC) value in an associated routing pattern when attempted calls utilizing the data module fail to complete. The BCC values must be the same. For a detailed description of BCC and their ability to provide specialized routing for various types of voice and data calls, see <i>Avaya Aura® Communication Manager Feature Description and Implementation</i>. The BCC value is used to determine compatibility when non-ISDN-PRI facilities are connected to ISDN facilities (ISDN-PRI Interworking).</p> <p>The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>1</b>: Relates to 56-kbps</li> <li>• <b>2, 3, 4</b>: Relates to 64 kbps</li> </ul> |
| <b>Broadcast Address</b>      | Used with Ethernet data modules. Does not appear for S87XX Series IP-PNC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Connected Data Module</b>  | This is the data module extension to which the link connects. Used with Processor Interface (used with DEFINITY CSI only) data modules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Connected to</b>           | <p>The Asynchronous Data Unit (ADU) to which the system is connected to. Used with Data Line and Processor/Trunk (pdm selection) Data Module.</p> <p>The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>dte</b>: Data Terminal Equipment. Used with Data Line and Processor/Trunk Data Modules.</li> <li>• <b>isn</b>: Information Systems Network. Used with Data Line and Processor/Trunk Data Modules.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Class Of Service</b>       | The desired class of service. Does not appear for Ethernet. The valid entries range from <b>0</b> to <b>15</b> to select the allowed features.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Class Of Restriction</b>   | The desired class of restriction. Does not appear for Ethernet. The valid entries range from <b>0</b> to <b>999</b> to select the allowed restrictions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Extension</b>              | Indicates the extension assigned to the data module. This is a display-only field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Enable Link</b>            | Used with Point-to-Point and Processor Interface data modules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Establish Connection</b>   | Used with Point-to-Point, and Processor Interface (used with DEFINITY CSI only) data modules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>IP Address Negotiation</b> | Used with Point-to-Point data modules. Does not appear for S87XX Series IP-PNC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Table continues...

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ITC</b>                  | <p>Information Transfer Capability. Indicates type of transmission facilities to be used for ISDN calls originated from this endpoint. Appears only when, on the Trunk Group screen, the Comm Type field is 56k-data or 64k-data. Does not display for voice-only or BRI stations. Used with 7500, Announcement, data-line, Netcon, Processor/Trunk (pdm selection), Processor Interface, and System Port Data Modules.</p> <p>The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>restricted</b>: Either restricted or unrestricted transmission facilities are used to complete the call. A restricted facility is a transmission facility that enforces 1's density digital transmission (that is, a sequence of eight digital zeros is converted to a sequence of 7 zeros and a digital 1).</li> <li>• <b>unrestricted</b>: Only unrestricted transmission facilities are used to complete the call. An unrestricted facility is a transmission facility that does not enforce 1's density digital transmission (that is, digital information is sent exactly as is).</li> </ul> |
| <b>Link</b>                 | <p>A communication interface link number. Used with Ethernet, Point-to-Point, and Processor Interface (used with DEFINITY CSI only) data modules. This field is in different locations on the screen for different data module types. The valid entries range from <b>0</b> to <b>99</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Extension</b>            | <p>The extension number required to perform maintenance functions on the standby Netcon physical channel in a duplicated system. The standby remote loop around tests fails if this field is not administered. Used with Netcon and Processor Interface Data Modules.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>MM Complex Voice Ext</b> | <p>This field contains the number of the associated telephone in the multimedia complex. This field appears only after you set the Multimedia field to <u>y</u>. This field is left blank until you enter the data module extension in MM Complex Data Ext on the Station screen. Used with 7500 and World Class BRI Data Modules. Does not appear on S87XX Series IP-PNC. Valid entries are valid values that conform to your dial plan. After you complete the field on the Station screen, the two extensions are associated as two parts of a one-number complex, which is the extension of the telephone.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Multimedia</b>           | <p>Used with the 7500 and World Class BRI Data Modules. Appears only if, on the System Parameters Customer-Options (Optional Features) screen, the MM field is <u>y</u>. You can select this option to make this data module part of a multimedia complex.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

*Table continues...*

| Name                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                                     | <p>The name of the user associated with the data module. The name is optional and can be blank. It can contain up to 27 alphanumeric characters.</p> <p> <b>Note:</b></p> <p>Avaya BRI stations support ASCII characters only. BRI stations do not support non-ASCII characters, such as Eurofont or Kanafont. Therefore, if you use non-ASCII characters in any Communication Manager Name field, such characters do not display correctly on a BRI station.</p>                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Network uses 1's for Broadcast Addresses</b> | Indicates that a broadcast address is used to send the same message to all systems or clients on a local area network. Used with Ethernet data modules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Node Name</b>                                | Appears when the Data Module type is ppp. Used with Ethernet (not on S87XX Series IP-PNC) and Point-to-Point data modules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>PDATA Port</b>                               | <p>Used to relate the physical PDATA port to which the mode 3 portion of the system port is connected. You need to enter a seven-digit alphanumeric port location to which the data module is connected. This entry must be assigned to a port on a PDATA Line Board. Used with System Port Data Modules.</p> <p>The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>01 to 22:</b> First and second characters are the cabinet numbers</li> <li>• <b>01 to 64:</b> First and second characters are the cabinet numbers (S87XX Series IP-PNC)</li> <li>• <b>A to E:</b> Third character is the carrier</li> <li>• <b>01 to 20:</b> Fourth and fifth characters are the slot numbers in the carrier</li> <li>• <b>01 to 12:</b> Sixth and seventh characters are the circuit numbers</li> </ul>                                                                                                                 |
| <b>Physical Channel</b>                         | <p>The Physical Channel number is referred to on associated system forms as the Interface Link number. Used with Netcon and Processor Interface Data Modules.</p> <p>The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>01 to 08:</b> For Processor Interface Data Modules, enter the 2-digit circuit number of the Processor Interface port. A multi-carrier cabinet system supports the use of two Processor Interface circuit packs, the first circuit pack (mounted in Control Carrier A) supports physical channels or links 01 through 04; the second (mounted in Control Carrier A) supports physical channels or links 05 through 08. A single-carrier cabinet system supports one Processor Interface circuit pack and physical channels or links 01 through 04 only.</li> <li>• <b>01 to 04:</b> For DEFINITY CSI configurations. For Netcon Data Modules, enter a netcon data channel.</li> </ul> |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Loop-Around Test</b> | Indicates whether data module supports a loop-back test at the EIA interface. Appears when the Data Module Type field is set to <code>pdm</code> or <code>tdm</code> . Used with Processor/Trunk Data Modules. In general, Avaya equipment supports this test but it is not required by Level 2 Digital Communications Protocol. To abort a request for this test, you may clear this check box. |
| <b>Secondary Data Module</b>   | Indicates that this PDM is the secondary data module used for Dual I-channel AUDIX networking. Appears only when the Type field is <code>pdm</code> . Used with Processor/Trunk Data Modules. The primary data module must be administered before the secondary data module can be added. If the Port field entry is <code>x</code> , then do not select the Secondary Data Module option.       |
| <b>Subnet Mask</b>             | A 32-bit binary number that divides the network ID and the host ID in an IP address. Used with Point-to-Point data modules (for S87XX Series IP-PNC).                                                                                                                                                                                                                                            |
| <b>Tenant Number</b>           | Determines the music source for callers on hold. Valid entries range from <b>0</b> through <b>100</b> .                                                                                                                                                                                                                                                                                          |

**Board:** Displays the five-character announcement circuit pack number that identifies the physical circuit pack to which the announcement module is connected. You can enter `x` in this field to indicate that there is no hardware associated with this port assignment. Used with Announcement Data Modules.

The five-character announcement board number consists of:

| Characters    | Meaning          | Value                                |
|---------------|------------------|--------------------------------------|
| <b>1 to 2</b> | Cabinet Number   | <b>1 to 64</b> (S87XX Series IP-PNC) |
| <b>3</b>      | Carrier          | <b>A to E</b>                        |
| <b>4 to 5</b> | Slot Number or X | <b>0 to 20</b>                       |

**Port:** Specifies a port location to which the data module is connected. Used with 7500, Data Line, Ethernet, Processor/Trunk, PPP, System Port, and World Class BRI Data Modules.

 **Note:**

You can enter `x` in the Port field to indicate that there is no hardware associated with the port assignment, also known as Administration Without Hardware (AWOH). These stations are referred to as phantom stations. If this data module is designated as a secondary data module, that is secondary data module is set to `y`, you cannot enter `x` in this field. You cannot change the port of a primary data module to `x` if a secondary data module is administered.

| Characters    | Meaning        | Value                                |
|---------------|----------------|--------------------------------------|
| <b>1 to 2</b> | Cabinet Number | <b>1 to 64</b> (S87XX Series IP-PNC) |
| <b>3</b>      | Carrier        | <b>A to E</b>                        |
| <b>4 to 5</b> | Slot Number    | <b>0 to 20</b>                       |

*Table continues...*

| Characters | Meaning        | Value                                                                                                                                                                                                                                                                                                   |
|------------|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6 to 7     | Circuit Number | <ul style="list-style-type: none"> <li>• <b>01 to 31</b> (S87XX Series IP-PNC (tdm, pdm) configurations)</li> <li>• <b>01 to 16</b> (ppp for S87XX Series IP-PNC)</li> <li>• <b>01 to 08</b> (system-port for S87XX Series IP-PNC)</li> <li>• <b>17/33</b> (Ethernet on S87XX Series IP-PNC)</li> </ul> |

**Data Module Type:** Displays the type of data module.

| Valid Entry         | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>7500</b>         | Assigns a 7500 Data Module. The 7500 data module supports automatic TEI, B-channel, maintenance and management messaging, and SPID initialization capabilities. BRI endpoints, both voice and/or data, are assigned to either the ISDN-BRI - 4-wire S/T-NT Interface circuit pack or the ISDN-BRI - 2-wire U circuit pack. Each can support up to 12 ports. Since BRI provides multipoint capability, more than one ISDN endpoint (voice or data) can be administered on one port. For BRI, multipoint administration allows for telephones having SPID initialization capabilities, and can only be allowed if no endpoint administered on the same port is a fixed tie endpoint and no station on the same port has B-channel data capability. Currently, multipoint is restricted to two endpoints per port. |
| <b>announcement</b> | Assigns an announcement data module. The announcement data module is built-in to the integrated announcement circuit pack and is administered using the Announcement Data Module screen. This data module allows the system to save and restore the recorded announcements file between the announcement circuit pack and the system memory.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

*Table continues...*

| Valid Entry      | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>data-line</b> | <p>Assigns a Data Line Data Module. The Data Line Data Module (DLDM) screen assigns ports on the Data Line circuit pack (DLC) that allows EIA 232C devices to connect to the system. The DLC, with a companion Asynchronous Data Unit (ADU), provides a less expensive data interface to the system than other asynchronous DCP data modules. The DLC supports asynchronous transmissions at speeds of Low and 300, 1200, 2400, 4800, 9600, and 19200 bps over 2-pair (full-duplex) lines. These lines can have different lengths, depending on the transmission speed and wire gauge. The DLC has 8 ports. The connection from the port to the EIA device is direct, meaning that no multiplexing is involved. A single port of the DLC is equivalent in functionality to a data module and a digital line port. The DLC appears as a data module to the Digital Terminal Equipment (DTE) and as a digital line port to the server running Communication Manager. The DLC connects the following EIA 232C equipment to the system:</p> <ul style="list-style-type: none"> <li>• Printers</li> <li>• Non-Intelligent Data Terminals</li> <li>• Intelligent Terminals, Personal Computers</li> <li>• Host Computers</li> <li>• Information Systems Network (ISN), RS-232C Local Area Networks (LANs), or other data switches</li> </ul> |
| <b>ethernet</b>  | <p>The name associated with an endpoint. The name you enter displays on called telephones that have display capabilities. In some messaging applications, such as Communication Manager Messaging, you can enter the user name (last name first) and their extension to identify the telephone. The name you enter is also used for the integrated directory.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>ni-bri</b>    | <p>Assigns an NI-BRI Data Module.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

*Table continues...*

| Valid Entry        | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>pdm</b>         | Assigns a DCE interface for Processor/Trunk Data Modules. These screens assign Modular Processor Data Modules (MPDMs) and Modular Trunk Data Modules (MTDMs). One screen is required for assigning MPDMs (700D), 7400B, 7400D or 8400B Data Module, and another screen for MTDMs (700B, 700C, 700E, 7400A). One screen must be completed for each MPDM, 7400B, 7400D, 8400B or MTDM. The MPDM, 7400B, or 8400B Data Module provides a Data Communications Equipment (DCE) interface for connection to equipment such as data terminals, CDR output devices, on-premises administration terminal, Message Server, Property Management System (PMS), AUDIX, and host computers. It also provides a Digital Communications Protocol(DCP) interface to the digital switch. (DCE is the equipment on the network side of a communications link that provides all the functions required to make the binary serial data from the source or transmitter compatible with the communications channel.) The MTDM provides an Electronic Industries Association (EIA) Data Terminal Equipment (DTE) interface for connection to off-premises private line trunk facilities or a switched telecommunications network and a DCP interface for connection to the digital switch. (DTE is the equipment comprising the endpoints in a connection over a data circuit. For example, in a connection between a data terminal and a host computer, the terminal, the host, and their associated modems or data modules make up the DTE.) The MTDM or 7400A Data Module also can serve as part of a conversion resource for Combined Modem Pooling. |
| <b>ppp</b>         | Assigns a Point-to-Point Protocol data module. The PPP Data Module screen assigns a synchronous TCP/IP port on the Control Lan (C-Lan) circuit pack. These ports are tailored to provide TCP/IP connections for use over telephone lines. For more information on Point-to-Point data modules, see <i>Administering Network Connectivity on Avaya Aura® Communication Manager</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>system-port</b> | Assigns a System Port Data Module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>tdm</b>         | Assigns a DTE interface for Processor/Trunk Data Modules. See the pdm entry above.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>wcbri</b>       | Assigns a World Class BRI Data Module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Performs the action you initiate.                                   |
| <b>Schedule</b> | Performs the action at the specified time.                          |
| <b>Reset</b>    | Clears the action and resets the fields.                            |
| <b>Clear</b>    | Clears all entries.                                                 |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>      | Performs the action you initiate real time.                         |

---

## Class of service

### Class Of Service

Class Of Service (COS) allows you to administer permissions for call processing features that require dial code or feature button access. COS determines the features that can be activated by or on behalf of endpoints. Using System Manager you can view and modify the Class Of Service data.

### Editing Class Of Service data

#### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. In the navigation pane, click **System > Class of Service**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Class Of Service that you want to edit.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields and click **Commit** to save the changes.

#### Related links

[Class of Service field descriptions](#) on page 815

### Viewing Class Of Service data

#### Procedure

1. On the System Manager web console, click **Elements > Messaging**.
2. In the navigation pane, click **System > Class of Service**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Select the Class Of Service you want to view.
6. Click **View** to view the Class Of Service data.

#### Related links

[Class of Service field descriptions](#) on page 815

### Filtering the Class Of Service list

#### Procedure

1. On the System Manager web console, click **Elements > Messaging**.



2. In the navigation pane, click **System > Class of Service**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Filter: Enable** in the Class Of Service List.
6. Filter the list according to one or multiple columns.
7. Click **Apply**.

To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

 **Note:**

The table displays only those options that match the filter criteria.

## Class of Service field descriptions

| Name          | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| <b>System</b> | The name of the Communication Manager associated with the Class of Service. |
| <b>Number</b> | The Class of Service number.                                                |

### General options

| Name                             | Description                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ad-hoc video conferencing</b> | Enables Ad-hoc Video Conferencing, so that up to six users can participate in a video conference call.                                                                                                                                                                                                                                            |
| <b>Automatic Callback</b>        | Allows users to request Automatic Callback.                                                                                                                                                                                                                                                                                                       |
| <b>Automatic Exclusion</b>       | Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.                                                                                                                                                                                                                     |
| <b>Buttonless Auto Exclusion</b> | Allows bridged appearances to operate in the exclusion mode regardless of the existence of an administered exclusion button. Currently this feature is only administrable on a per-endpoint basis by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.                                      |
| <b>Call Forwarding Busy / DA</b> | Allows users to forward calls to any extension when the dialed extension is busy or does not answer.                                                                                                                                                                                                                                              |
| <b>Call Forwarding Enhanced</b>  | Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.                                                                                                                                                                                                                |
| <b>Call Forwarding All Calls</b> | Allows users to forward all calls to any extension.                                                                                                                                                                                                                                                                                               |
| <b>Client Room</b>               | Allows users to access Check-In, Check-Out, Room Change/Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message waiting notification. You can administer class of service for Client Room only when you have Hospitality Services and a Property Management System interface. |

*Table continues...*

| Name                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Conference Tones</b>              | <p>This feature provides the conference tone as long as three or more calls are in a conference call.</p> <p>If you enable these tones for countries other than Italy, Belgium, United Kingdom, or Australia, the tones will be equivalent to no tone (silence) unless the tone is independently administered or customized on the Tone Generation screen.</p>                                                                                                                                                                                                                                                                                                                                                     |
| <b>Console Permissions</b>           | <p>Allows multi-appearance telephone users to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or motel, or to a call center supervisor. With console permission, a user can:</p> <ul style="list-style-type: none"> <li>• Activate Automatic Wakeup for another extension</li> <li>• Activate and deactivate controlled restrictions for another extension or group of extensions</li> <li>• Activate and deactivate Do Not Disturb for another extension or group of extensions</li> <li>• Activate Call Forwarding for another extension</li> <li>• Add and remove agent skills</li> <li>• Record integrated announcements</li> </ul> |
| <b>Contact Closure Activation</b>    | Allows a user to open and close a contact closure relay.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Data Privacy</b>                  | Isolates a data call from call waiting or other interruptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>MOC Control</b>                   | The option to assign administrative control on Microsoft Office Communicator (MOC) for either of the 0-15 entries on COS or COS Group objects. By default, this check box is clear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Bridging Exclusion Override</b>   | Allows a station to bridge on a call that has exclusion activated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Extended Forwarding All</b>       | Allows a user to administer call forwarding (for all calls) from a remote location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Extended Forwarding Busy / DA</b> | Allows this user to administer call forwarding (when the dialed extension is busy or does not answer) from a remote location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Intra-Switch CDR</b>              | Administers extensions for which Intra-Switch CDR is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Masking CPN / Name Override</b>   | Allows users to override the MCSNIC capability (that is, masking the display of calling party information and replacing it with a hard-coded, system-wide text string, Info Restricted).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Off-Hook Alert</b>                | To enable this option, either the Hospitality (Basic) or Emergency Access to Attendant field must be enabled in your license file. When enabled, these fields display as y on the System- Parameters Customer-Options screen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

*Table continues...*

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personal Station Access (PSA)</b>  | Allows users to associate a telephone to their extension with their programmed services, using a feature access code. This field must be set to n for virtual telephones. This field must be set to y at a user's home endpoint in order for that user to use the Enterprise Mobility User (EMU) feature at other endpoints.                                         |
| <b>Priority Calling</b>               | Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override send all calls, if active.                                                                                                                                                                                                                         |
| <b>Priority IP Video</b>              | Allows priority video calling, where video calls have an increased likelihood of receiving bandwidth and can also be allocated a larger maximum bandwidth per call.                                                                                                                                                                                                  |
| <b>QSIG Call Offer Originations</b>   | Allows users to invoke QSIG Call Offer services.                                                                                                                                                                                                                                                                                                                     |
| <b>Restrict Call Fwd-Off Net</b>      | Restricts users from forwarding calls to the public network. For security reasons, this should be enabled for all classes of service except the ones you use for very special circumstances.                                                                                                                                                                         |
| <b>Trk-To-Trk Transfer Override</b>   | Users with this COS override any system and/or COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for users with this COS.                                                                                                                                                                                    |
| <b>VIP Caller</b>                     | Enables automatic priority calling when assigned to the originator of a call. A call from a VIP phone is always a priority call without the use of a feature button or FAC.                                                                                                                                                                                          |
| <b>Match BCA Display to Principal</b> | The format of the incoming calls on the bridged call appearances of a COS Group. The possible values are: <ul style="list-style-type: none"> <li>• <b>y</b>: Displays the incoming call in the &lt;calling name/number&gt; format</li> <li>• <b>n</b>: Displays the incoming call in the &lt;calling name/number&gt; to &lt;principal station&gt; format.</li> </ul> |

| Button        | Description                                                    |
|---------------|----------------------------------------------------------------|
| <b>Commit</b> | Saves the changes you make.                                    |
| <b>Reset</b>  | Undoes the changes you made.                                   |
| <b>Edit</b>   | Takes you to the Edit Class of Service data page.              |
| <b>Done</b>   | Performs the action you initiate.                              |
| <b>Cancel</b> | Cancels the current action and takes you to the previous page. |

## Authorization Code

### Authorization Code

Use authorization code to control the calling privileges of system users. Authorization codes extend control of calling privileges and enhance security for remote access callers. You can use authorization codes to:

- Override a facilities restriction level (FRL) that is assigned to an originating station or trunk

- Restrict individual incoming tie trunks and remote access trunks from accessing outgoing trunks
- Track Call Detail Recording (CDR) calls for cost allocation
- Provide additional security control

## Authorization Code List

Authorization Code List displays all the authorization codes under the Communication Manager you select. You can apply filters and sort each column in the Authorization Code List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                        | Description                                                                   |
|-----------------------------|-------------------------------------------------------------------------------|
| <b>Authorization Code</b>   | The authorization code, which is a combination of 4 to 13 digits.             |
| <b>Class of Restriction</b> | The associated Class Of Restriction.                                          |
| <b>System</b>               | The name of the Communication Manager associated with the authorization code. |

## Viewing Authorization Code

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Authorization Code**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Authorization Code List, select the authorization code you want to view.
6. Click **View**.

### Related links

[Authorization Code field descriptions](#) on page 819

## Editing Authorization Code

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Authorization Code**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Authorization Code List, select the authorization code you want to edit.
6. Click **Edit** or click **View > Edit**.

7. Edit the required fields on the **Edit Authorization Code** page.
8. Click **Commit** to save the changes.

#### Related links

[Authorization Code field descriptions](#) on page 819

### Authorization Code field descriptions

| Name                      | Description                                                                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authorization Code</b> | Displays a combination of 4 to 13 digits. The number of digits must agree with the number assigned to the Authorization Code Length field on the Feature-Related System Parameters screen. To enhance system security, choose Authorization Codes of 13 random digits. |
| <b>COR</b>                | Displays the Class Of Restriction. Valid entry ranges from <b>0</b> to <b>95</b> . When a user dials the associated authorization code, this is the COR that the telephone or other facility will assume for that call.                                                |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Performs the action you initiate.                                   |
| <b>Schedule</b> | Performs the action at the specified time.                          |
| <b>Reset</b>    | Clears the action and resets the fields.                            |
| <b>Clear</b>    | Clears all entries.                                                 |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>      | Performs the action you initiate real time.                         |

---

## Class of Service Group

### Class Of Service Group

With Class Of Service Group, you can view the list of up to 100 Class Of Service (COS) groups on the screen. You can also change the configuration of individual COS group properties and edit up to 15 COS options within a group.

### Class Of Service Group List

Class Of Service Group List displays the groups of Class Of Service under the Communication Manager you select. You can apply filters and sort each of the columns in the Class Of Service Group List.

When you click **Refresh**, you can view the updated information available after the last synchronization operation.

| Name                | Description                                                                       |
|---------------------|-----------------------------------------------------------------------------------|
| <b>Group Number</b> | The number of the Class Of Service group. The group number ranges from 1 to 100.  |
| <b>Group Name</b>   | The name of the Class Of Service group.                                           |
| <b>System</b>       | The name of the Communication Manager associated with the Class Of Service Group. |

## Viewing Class Of Service Group

You can view the list of up to 100 Class of Service (COS) groups on this screen.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Class of Service Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Class Of Service Group List, select the group number for which you want to view the data.
6. Click **View**.

### Related links

[Class Of Service Group field descriptions](#) on page 821

## Editing Class Of Service Group

You can change the configuration of individual Class Of Service (COS) group properties and edit up to 15 COS options within a group on this screen.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Class of Service Group**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. From the Class Of Service Group List, select the group number for which you want to edit the data.
6. Click **Edit** or click **View > Edit**.
7. Edit the required fields on the **Edit Class Of Service Group Data** page.
8. Click **Commit** to save the changes.

## Related links

[Class Of Service Group field descriptions](#) on page 821

## Class Of Service Group field descriptions

| Name                             | Description                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                    | The name of the Communication Manager associated with the Class Of Service.                                                                                                                                                                                                                                                                      |
| <b>Group Number</b>              | The Class Of Service number. The group number can range from <b>1</b> to <b>100</b> . This field appears when, on the System Parameters Customer-Options (Optional Features) screen, the <b>Tenant Partitioning</b> field is set to <i>y</i> .                                                                                                   |
| <b>Group Name</b>                | The name of the Class Of Service Group. This field appears when, on the System Parameters Customer-Options (Optional Features) screen, the <b>Tenant Partitioning</b> field is set to <i>y</i> .                                                                                                                                                 |
| <b>Ad-hoc video conferencing</b> | Enables the ad-hoc video conference capability. Six users can participate in a video conference call.                                                                                                                                                                                                                                            |
| <b>Automatic Callback</b>        | Allows users to request Automatic Callback.                                                                                                                                                                                                                                                                                                      |
| <b>Automatic Exclusion</b>       | Allows a user to activate automatically Exclusion when they go off hook on an endpoint that has an assigned Exclusion button.                                                                                                                                                                                                                    |
| <b>Buttonless Auto Exclusion</b> | Allows bridged appearances to operate in the exclusion mode regardless of the existence of an administered exclusion button. Currently this feature is only administrable on a per-endpoint basis by administering a feature exclusion button. This feature relaxes the requirement to use a feature button.                                     |
| <b>Call Forwarding Busy / DA</b> | Allows users to forward calls to any extension when the dialed extension is busy or does not answer.                                                                                                                                                                                                                                             |
| <b>Call Forwarding Enhanced</b>  | Allows users to designate different preferred destinations for forwarding calls that originate from internal and external callers.                                                                                                                                                                                                               |
| <b>Call Forwarding All Calls</b> | Allows users to forward all calls to any extension.                                                                                                                                                                                                                                                                                              |
| <b>Client Room</b>               | Allows users to access Check-In, Check-Out, Room Change/ Swap, and Maid status functions. In addition, Client Room is required at consoles or telephones that are to receive message waiting notification. You can administer COS for Client Room only when you have Hospitality Services and a Property Management System interface.            |
| <b>Conference Tones</b>          | This feature provides the conference tone as long as three or more calls are in a conference call. If you enable these tones for countries other than Italy, Belgium, United Kingdom, or Australia, the tones will be equivalent to no tone (silence) unless the tone is independently administered or customized on the Tone Generation screen. |

*Table continues...*

| Name                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Console Permissions</b>           | <p>Allows multi-appearance telephone users to control the same features that the attendant controls. You might assign this permission to front-desk personnel in a hotel or motel, or to a call center supervisor.</p> <p>With console permission, a user can:</p> <ul style="list-style-type: none"> <li>• Activate Automatic Wakeup for another extension</li> <li>• Activate and deactivate controlled restrictions for another extension or group of extensions</li> <li>• Activate and deactivate Do Not Disturb for another extension or group of extensions</li> <li>• Activate Call Forwarding for another extension</li> <li>• Add and remove agent skills</li> <li>• Record integrated announcements</li> </ul> |
| <b>Contact Closure Activation</b>    | Allows a user to open and close a contact closure relay.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Data Privacy</b>                  | Isolates a data call from call waiting or other interruptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Extended Forwarding All</b>       | Allows a user to administer call forwarding for all calls from a remote location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Extended Forwarding Busy / DA</b> | Allows this user to administer call forwarding when the dialed extension is busy or does not answer from a remote location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Intra-Switch CDR</b>              | Administers extensions for which Intra-Switch CDR is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Masking CPN / Name Override</b>   | Allows users to override the MCSNIC capability, that is, masking the display of calling party information and replacing it with a hard-coded, system-wide text string, Info Restricted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Off-Hook Alert</b>                | To enable this option, either the Hospitality (Basic) or Emergency Access to Attendant field must be enabled in your license file. When enabled, these fields display as <b>y</b> on the System- Parameters Customer-Options screen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Personal Station Access (PSA)</b> | Allows users to associate a telephone to their extension with their programmed services, using a feature access code. This field must be set to <b>n</b> for virtual telephones. This field must be set to <b>y</b> at a user's home endpoint in order for that user to use the Enterprise Mobility User (EMU) feature at other endpoints.                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Priority Calling</b>              | Allows users to dial a feature access code to originate a priority call. Such calls ring differently and override Send All Calls, if active.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Priority IP Video</b>             | Allows priority video calling, where video calls have an increased likelihood of receiving bandwidth and can also be allocated a larger maximum bandwidth per call.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>QSIG Call Offer Originations</b>  | Allows users to invoke QSIG Call Offer services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Restrict Call Fwd- Off Net</b>    | Restricts users from forwarding calls to the public network. For security reasons, this should be enabled for all COS except the ones you use for very special circumstances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*



| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Trk-To-Trk Transfer Override</b>   | Users with this COS override any system and/or COR-to-COR calling party restrictions that would otherwise prohibit the trunk-to-trunk transfer operation for users with this COS.                                                                                                                                                                                    |
| <b>VIP Caller</b>                     | Enables automatic priority calling when assigned to the originator of a call. A call from a VIP phone is always a priority call without the use of a feature button or FAC.                                                                                                                                                                                          |
| <b>Match BCA Display to Principal</b> | The format of the incoming calls on the bridged call appearances of a COS Group. The possible values are: <ul style="list-style-type: none"> <li>• <b>y</b>: Displays the incoming call in the &lt;calling name/number&gt; format</li> <li>• <b>n</b>: Displays the incoming call in the &lt;calling name/number&gt; to &lt;principal station&gt; format.</li> </ul> |

| Button          | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <b>Commit</b>   | Performs the action you initiate.                                   |
| <b>Schedule</b> | Performs the action at the specified time.                          |
| <b>Reset</b>    | Clears the action and resets the fields.                            |
| <b>Clear</b>    | Clears all entries.                                                 |
| <b>Done</b>     | Completes your current action and takes you to the subsequent page. |
| <b>Cancel</b>   | Cancels your current action and takes you to the previous page.     |
| <b>Now</b>      | Performs the action you initiate real time.                         |

## Uniform Dial Plan Groups

### Uniform Dial Plan Group

A Uniform Dial Plan Group is a set of Communication Manager systems that use the Uniform Dialing Plan (UDP) feature. You can use the Uniform Dial Plan Groups capability in System Manager to create, view, modify, and delete uniform dial plan (UDP) groups.

### Adding a Uniform Dial Plan Group

#### About this task

Use this page to create a new UDP Group. While creating a new UDP Group, make sure that the Communication Manager systems you select share common extension ranges.

#### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Click **System > Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, click **New**.

4. On the Add UDP Group page, enter the name for the UDP Group you want to create in the **Group Name** field.
5. Select the **Auto Update All** check box if you want the UDP tables of every Communication Manager system that you add to this group to be updated automatically.
6. Select the **Create local UDP table entry** check box if you want to create a local entry automatically in the UDP table of the Communication Manager system when you add an endpoint to it.
7. Enter the required information in the fields under the **Group Members** and **Group Ranges** tabs.
8. Click **Commit**.
9. On the System Manager console, click **Groups & Roles > Groups** to verify that the system added the group with the same name and resources.

#### Related links

[Add UDP Groups field descriptions](#) on page 825

## Editing a Uniform Dial Plan Group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Click **System > Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to modify from the UDP Group List.
4. Click **Edit**.
5. On the Edit UDP Groups page, modify the required fields.
6. Click **Commit**.

#### Related links

[Add UDP Groups field descriptions](#) on page 825

## Viewing a Uniform Dial Plan Group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Click **System > Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to view from the UDP Group List.
4. Click **View**. The system displays the **View UDP Group** page.

#### Related links

[Add UDP Groups field descriptions](#) on page 825

## Deleting a Uniform Dial Plan Group

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. Click **System > Uniform Dial Plan Groups** in the left navigation pane.
3. On the UDP Groups page, select the UDP Group that you want to delete from the UDP Group List.
4. Click Delete.

### Related links

[Add UDP Groups field descriptions](#) on page 825

## Add UDP Groups field descriptions

| Name                                | Description                                                                                                                                                                                                  |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group Name</b>                   | To enter a name for the UDP group that you want to create.                                                                                                                                                   |
| <b>Auto Update All</b>              | To automatically update the UDP tables of every Communication Manager that you add to this group.                                                                                                            |
| <b>Create local UDP table entry</b> | To create a local entry automatically in the UDP table of the Communication Manager system when you add an endpoint.                                                                                         |
| <b>Update on Sync</b>               | During Communication Manager Sync, if System Manager finds any new extension within the UDP Group ranges, then System Manager updates the UDP table of all Communication Manager that are in that UDP group. |

### Group Members

| Name                    | Description                                                                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CM Systems</b>       | A list of Communication Manager systems from which you can select the Communication Manager that you want to add to the new UDP Group. A UDP Group can contain 2 to 10 systems. |
| <b>Add</b>              | The link to add one or more Communication Manager systems to the new UDP Group. Is this a field or a group member?                                                              |
| <b>Element Name</b>     | The name of the Communication Manager system that you added to the UDP group. This field is view only.                                                                          |
| <b>Software Version</b> | The version of the Communication Manager system that you added to the UDP group. This field is view only.                                                                       |
| <b>Remove</b>           | The link to remove the Communication Manager systems that you selected from the <b>CM Systems</b> field list.                                                                   |

### Group Ranges

| Name                    | Description                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>System Dial Plan</b> | A list of a common range of extensions available on the Communication Manager systems that you selected in the Group Members tab. |

*Table continues...*

| Name        | Description                                                                       |
|-------------|-----------------------------------------------------------------------------------|
| <b>From</b> | The starting range of extension numbers. The first extension number in the range. |
| <b>To</b>   | The closing range of extension number. The last extension number in the range.    |
| <b>Add</b>  | The link to add the specified range of extension numbers.                         |

## Group Range Configuration

| Name                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Range</b>          | The range of extension numbers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>UDP Type</b>       | Enter the initials of the call-processing server network that the system uses to analyze the converted number. Valid entries are <b>aar</b> , <b>ars</b> , and <b>ext</b> . First describe what is UDP type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Delete Digits</b>  | The number of digits that the software deletes before the software routes a call. Valid entries are <b>0</b> through <b>3</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Node/Location#</b> | The extension number portability (ENP) node number. Valid entries are <b>1</b> to <b>999</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Insert Digits</b>  | The specific digits or the number of administered location prefix digits inserted before routing the call. Select one of the following: <ul style="list-style-type: none"> <li>• 0 to 9 (1 to 4 digits): The digits that replace the deleted portion of the dialed number.</li> <li>• Lx (1 to 5): The variable x represents the number of digits between 1 and 5 and is the number of leading digits taken from the administered location prefix. These digits are followed by the dialed string. The number of digits in the location prefix must be more than x.</li> <li>• The field to specify the location prefix digits. Leave the Insert Digits field blank if you do not want to specify the location prefix digits.</li> </ul> |
| <b>Conv</b>           | The range configurations used to create the <b>Uniform Dial Plan</b> entries on Communication Manager when an extension in the common ranges is added.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Button        | Description                                                  |
|---------------|--------------------------------------------------------------|
| <b>Commit</b> | Performs the action that you start.                          |
| <b>Clear</b>  | Clears all entries.                                          |
| <b>Cancel</b> | Cancels the current action and reverts to the previous page. |

## Uniform Dial Plan

### Uniform Dial Plan field descriptions

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Matching Pattern</b> | The number that the Communication Manager instance uses to match the dialed numbers. You can enter up to 18 digits in the <b>Matching Pattern</b> field. You can also enter wildcard characters like x and X.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Length</b>           | The length of the dialed string for each type of call.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Del</b>              | The number of digits the system must delete from the initial digits of the dialed string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Insert Digits</b>    | <p>The specific digits or number of administered location prefix digits inserted before routing the call. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>0 to 9 (1 to 4 digits)</b>: The digits that replace the deleted portion of the dialed number.</li> <li>• <b>Lx (1 to 5)</b>: The variable x represents the number of digits between 1 and 5 and is the number of leading digits taken from the administered location prefix. These digits are followed by the dialed string. x must be less than the number of digits in the location prefix.</li> <li>• <b>blank</b>: Leave the <b>Insert Digits</b> field blank if you do not want to specify the location prefix digits.</li> </ul> |
| <b>Net</b>              | <p>The method that the call-processing server network uses to analyze the converted number. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>ext</b>: If you use this option, the call-processing server network analyzes the converted digit-string as an extension number.</li> <li>• <b>aar</b>: If you use this option, the call-processing server network analyzes the converted digit-string as an AAR address.</li> <li>• <b>ars</b>: If you use this option, the call-processing server network analyzes the converted digit-string as an ARS address.</li> </ul>                                                                                                                         |
| <b>Conv</b>             | The field that enables additional digital conversion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Node Number</b>      | <p>The destination node number in a private network when the system uses node number routing or Distributed Communication System (DCS). The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>blank</b>: Use this option if you do not want to enter the destination node number. This is the default option.</li> <li>• <b>1 to 999</b>: Use this option to enter the destination node number.</li> </ul>                                                                                                                                                                                                                                                                                                 |
| <b>System</b>           | The name of the Communication Manager system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Button     | Description       |
|------------|-------------------|
| <b>New</b> | Adds UDP entries. |

*Table continues...*

| Button                    | Description                            |
|---------------------------|----------------------------------------|
| <b>Edit</b>               | Edits the UDP entry you select.        |
| <b>View</b>               | Displays the details of the UDP entry. |
| <b>Update UDP Entries</b> | Updates UDP entries.                   |

## Adding UDP entries

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Uniform Dial Plan**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **New**.
6. Type a qualifier in the **Enter Qualifier** field.
7. Click **Add(+)**.
8. On the SAT screen, type the details of the UDP entry.
9. Click **Enter**.

The system adds the UDP entry to the UDP table.

## Viewing UDP entries

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Uniform Dial Plan**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Choose the UDP entry you want to view.
6. Click **View**.

The system displays the SAT screen with the details of the UDP entry.

## Editing UDP entries

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Uniform Dial Plan**.
3. Select one or more Communication Manager instance from the Communication Manager list.

4. Click **Show List**.
5. Select the UDP entry you want to edit.
6. Click **Edit**.
7. On the SAT screen, edit the details for the UDP entry.
8. Click **Enter**.

The system displays the status that the UDP was successfully edited on the UDP page.

## Update UDP entries

Use **Update UDP entries** to add or delete an extension as an endpoint extension on any Communication Manager instance in the UDP group. The extension is then added or deleted in the UDP of that Communication Manager instance and as an AAR or ARS in the UDP of other Communication Manager instances in the UDP group.

## Updating UDP entries

### Before you begin

You must configure at least one UDP group before you update the UDP entries.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **System > Uniform Dial Plan**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click **Update UDP Entries**.
6. Complete the Update UDP Entries page.
7. Click **Commit**.

### Related links

[Updating UDP entries field descriptions](#) on page 830

## Updating UDP entries field descriptions

| Name                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Update Mode</b>   | <p>The mode by which you want to select the extensions for updating the UDP entries. The choices are:</p> <ul style="list-style-type: none"> <li>• <b>File Upload:</b> Select this option if you want to upload a .txt file with extensions. You can either enter comma separated values or individual extensions in the text file.</li> <li>• <b>Select Extension:</b> Select this option to choose an extension range from the text box. You can also enter the extensions manually.</li> </ul>                                                                                                                                                                                        |
| <b>Operation</b>     | <p>The add or delete operation you want to perform on the UDP entries.</p> <ul style="list-style-type: none"> <li>• <b>Add:</b> Select <b>Add</b> to add an extension as an endpoint extension on any Communication Manager of the UDP group. The extension is then added in the UDP of that Communication Manager . The extension is also added as an AAR or ARS in the UDP of other Communication Managers in the UDP group.</li> <li>• <b>Delete:</b> Select <b>Delete</b> to delete an extension from the UDP of all the Communication Managers in the UDP group. The extension you want to delete must be present in one of the Communication Managers in the UDP group.</li> </ul> |
| <b>Select a File</b> | Click <b>Select a File</b> to browse to the text file in your local computer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Schedule Job</b>  | <p>The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Run immediately:</b> Select this option to update the UDP entries immediately.</li> <li>• <b>Schedule later:</b> Select this option to update the UDP entries at the scheduled time.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                              |

| Button        | Description                                              |
|---------------|----------------------------------------------------------|
| <b>Commit</b> | Updates the UDP entries for the UDP groups you selected. |
| <b>Cancel</b> | Cancels the update action.                               |

### Related links

[Updating UDP entries](#) on page 829

## Assigning permission to gain access UDP groups across Communication Manager instances

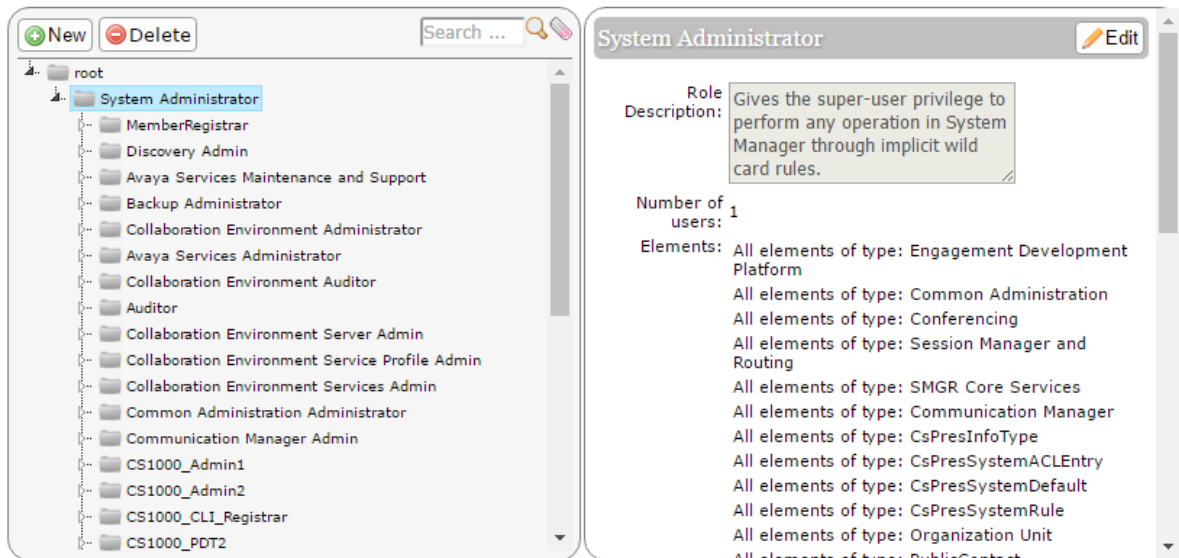
### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
  - Click **New**



- Right-click and select **New**.

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, click **UDP Group**.
9. Click **Next**.
10. On the Permission Mapping page, apply the required permissions. For example, select **Edit**.
11. Click **Commit**.

## Usage options

### Endpoint options

Use **Usage Options** to add and remove internal dependencies to an endpoint. Use **Add Options** to add references of an endpoint to other endpoint related objects such as Intra Switch CDR Agent, Intra Switch CDR Endpoint, and Intra Switch CDR VDN. If you select **Add Options** and add an endpoint, the system updates the reference objects you selected automatically.

For example, if you select **Intra Switch CDR for Endpoints** and add a new entry in endpoints, the same entry is added on the Intra Switch CDR form. The system displays **station-user** in the **Type** field.

Use **Usage Options** to:

- Add dependencies between an endpoint and Intra-Switch CDR for Agent, Endpoint, and VDN.
- Remove this endpoint from the bridged extension of another station, if configured.
- Remove an endpoint from a hunt group.
- Remove an endpoint from an Intra-switch CDR, if configured.
- Remove an Off-PBX-Telephone Endpoint-Mapping for the endpoint, if configured.
- Remove an endpoint from another the **Team** button of another endpoint, if configured.
- Remove an endpoint from the **Port Extension** field on the Agents form, if configured.
- Remove an endpoint from the Vector steps, if configured.
- Clear the voice messages that are waiting by selecting the **Clear AMW** checkbox.

 **Note:**

If an endpoint is referenced elsewhere and if you try to delete the endpoint, the Communication Manager gives an error. You must remove the reference before you delete the endpoint. You can remove the references using **Usage Option**.

## Related links

[Re-Calculate route pattern](#) on page 832

## Re-Calculate route pattern

You can update the route pattern based on the associated Session Manager.

On the Re-Calculate Route Pattern page, you can apply the changes to the endpoint that might have a Route Pattern value different from the value calculated based on Session Manager to route pattern association. The Select devices from Communication Manager List section provides a list of Communication Manager systems from where you can select Communication Manager.

The Session Manager Route Pattern association section is display only and contains the primary Session Manager and secondary Session Manager to Route Pattern association.

The Users with Administered Route Pattern different from Calculated Route Pattern section contains the users with a Route Selection different from the calculated Route Selection. You can select users and apply the changes by using **Apply Recalculate Route Pattern**. The system triggers a job that can run immediately or schedule for later. When the job is complete, the system applies the changes to Communication Manager and updates the System Manager database.

In the Users with Administered Route Pattern different from Calculated Route Pattern section, you can recalculate, update users, and apply the changes to users:

- After System Manager upgrades to 7.0, and you have configured Communication Manager 7.0 route patterns, you can update users in bulk from the Re-Calculate Route Pattern page.

You can also enable the **Calculate Route Pattern** check box on **Manage Users > User Management > Communication Profile > CM Endpoint profile** page.

- After you make changes to the existing route patterns after the initial setup, you can apply the changes to the affected users.

#### Related links

[Endpoint options](#) on page 831

## Adding dependencies to an endpoint, agent, or VDN

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the navigation pane, click **Options > Usage Options**.
3. Click the **Add Options** tab.
4. Select one of the following options for a Communication Manager:
  - **Intra-Switch CDR for Agent** to add an Intra-Switch CDR dependency while adding an agent to that Communication Manager
  - **Intra-Switch CDR for Endpoint** to add an Intra-Switch CDR dependency while adding an endpoint on that Communication Manager.
  - **Intra-Switch CDR for VDN** to add an Intra-Switch CDR dependency while adding a VDN on that Communication Manager.
5. Click **Commit**.

To clear the settings you have chosen, click **Reset**.

## Removing references to an endpoint

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Options > Usage Options**.
3. In the **Remove Options** tab, select the references you want to remove for the endpoint.
4. Click **Commit**.

#### Related links

[Remove usage options field descriptions](#) on page 833

## Remove usage options field descriptions

| Name          | Description                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>System</b> | The name of the Communication Manager. Select the checkbox next to <b>System</b> to select all the Communication Managers. |

*Table continues...*

| Name                                      | Description                                                                                                                                                   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bridged Extension</b>                  | Select this checkbox to remove the reference between the bridged extension and the endpoint you choose.                                                       |
| <b>Hunt Group</b>                         | Select this checkbox to remove the reference between the huntgroup and the endpoint you choose.                                                               |
| <b>Intra-Switch CDR</b>                   | Select this checkbox to remove the reference between the Intra-Switch CDR and the endpoint you choose.                                                        |
| <b>Off- PBX Telephone Station-Mapping</b> | Select this checkbox to remove the reference between the Off-PBX Telephone Station-Mapping and the endpoint you choose.                                       |
| <b>Team Button</b>                        | Select this checkbox to remove the reference between the <b>Team</b> Button and the endpoint you choose.                                                      |
| <b>Clear AMW</b>                          | Select the Automatic Message Waiting checkbox to clear all the voice messages that are waiting.                                                               |
| <b>Port Extension</b>                     | The assigned extension for the AAS or a voice messaging port. This extension cannot be a Vector Directory Number (VDN) or an Agent LoginID. Default is blank. |
| <b>Vector</b>                             | Select this checkbox to remove the reference between the Vector and the endpoint you choose.                                                                  |

| Button        | Description                                                  |
|---------------|--------------------------------------------------------------|
| <b>Commit</b> | Click to apply the remove option for the options you select. |
| <b>Reset</b>  | Click to undo all the changes you made.                      |

## NRP Group

### Overview of NRP group

By using the Network Routing Policy (NRP) group, you can add or remove Communication Manager within the NRP group. Communication Manager of the NRP group can then create **Location** entries in Session Manager for the field **Controlled by this CM server** for that network region.

After you add Communication Manager to the NRP group, you can set the **Controlled by this CM server** field to **Yes** or **No**.

If you specify the IP Network Region for the field **Controlled by this CM server** value to **Yes**, the Session Manager location will generate with **IP Network Region**, **Name** and **IP Network Map** linked for that IP Network Region.

On the IP Network Region page, you can perform the following:

- In the **Details** column, you can either show or hide the **IP Network Maps**.
- You can edit the **Name** and **Controlled by this CM server** fields for the **IP Network Region** that you have selected.

 **Note:**

If Communication Manager 1, Communication Manager 2, and Communication Manager 3 are in an NRP group, and you set the **Controlled by this CM Server** field to **Yes** for the **IP Network Region X** for Communication Manager 1.

Where **IP Network Region X** can be any **IP Network Region** other than **IP Network Region 1**, as **IP Network Region 1** is an exception.

 **Important:**

You cannot set the **Controlled by this CM Server** field to **Yes** for Communication Manager 2, and Communication Manager 3 in **IP Network Region X** because the these two Communication Manager instances are a part of the same NRP group.

## NRP sync feature

By using the NRP synchronization feature, users with H.323 phones can move between offices and have appropriate E911 routing for their location.

For the NRP sync feature, ensure that the authoritative Communication Manager **IP Network Region** information is configured in the Session Manager routing table. A Communication Manager server is authoritative for a location if the location contains media gateways and SIP endpoints that are administered on that Communication Manager server.

Therefore, if you make any change to the **IP Network Map** for the **IP Network Region** that are controlled by Communication Manager, the updates are automatically detected. These updates are replicated to the corresponding **Location** entries in the Session Manager routing table.

## Creating NRP groups

### About this task

Perform this procedure to add or remove one or more Communication Manager instances from an NRP group. The Communication Manager instances that you select will be a part of the NRP group. These Communication Manager instances will be authoritative over specific **IP Network Regions**.

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Options > NRP Group**.
3. In the **NRP Group** table, select the Communication Manager instances that you want to add to an NRP group.
4. Click **Commit**.

The Communication Manager instances that you selected are now a part of the NRP group. When you add a Communication Manager instance to the NRP group, the system changes the correlation flag of **IP Network Region 1** to **Yes**, which means that Session Manager Location is created using **IP Network Region 1**.

## Managing NRP groups

### Procedure

1. On the System Manager web console, click **Elements > Communication Manager**.
2. In the left navigation pane, click **Network > IP Network Regions**.
3. Select the specific Communication Manager instance from the list of Communication Manager instances.

### Result

The IP Network Region page displays the **Details**, **Name**, and **Controlled by this CM Server** columns of that Communication Manager instance.

For more information, see Overview of NRP group.

### Next steps

#### Controlled by this CM Server validation:

**Controlled by this CM Server** field is available on the IP Network Region List page. **Controlled by this CM Server** disables the validation check in place for using the same **IP Network Region** across multiple Communication Managers which are part of the **NRP Group**. **Network Region 1** is an exception to this validation check.

Set the **iptcm.properties > disableAuthValidation** property for using the **Controlled by this CM Server** validation.

| iptcm.properties > disableAuthValidation value | Validation scope                                                                                                                                                                             |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| True                                           | You can set the value of the <b>Controlled by this CM Server</b> field to <b>Yes</b> for the same IP Network region on all Communication Manager servers that are part of <b>NRP Group</b> . |
| False                                          | You can set the value of the <b>Controlled by this CM Server</b> field to <b>Yes</b> only for IP Network region 1 on all Communication Manager servers that are part of <b>NRP Group</b> .   |

### Related links

[Overview of NRP group](#) on page 834

## Correlation between Communication Manager and Session Manager

- The **Controlled by this CM Server** has two values: **Yes** and **No**.
- To edit the **Name** of the Communication Manager that controls that **IP Network Region** for a Communication Manager instance, set **Controlled by this CM Server** to **Yes**.
- To create a correlated Session Manager **Location**, set **Controlled by this CM Server** of **IP Network Region** of a Communication Manager that is a part of **NRP Group** to **Yes**.
- If **Controlled by the CM Server** is changed from **Yes** to **No** then the Session Manager location entry is deleted by the system.

## Controlled by the CM Server to Yes

Setting **Controlled by the CM Server** to **Yes** on IP Network region page creates a location on Session Manager.

To verify the Session Manager location on System Manager web console, click **Elements > Routing > Locations**.

- The **Controlled by this CM Server** is set to **Yes** only if Session Manager location creation is successful at the Session Manager. On List IP Network Region page, click **Save**.
- The change in **Region Name** or **IP Network Map** of **IP Network Region** that has **Controlled by this CM server** set to **Yes** is displayed back in Session Manager when the update occurs in System Manager.

### **Note:**

In case of a conflict or mismatch with the **Name** field on Session Manager, the system logs an error and the **Name** field remains unchanged on Session Manager. The system raises an alarm.

## Correlation between Session Manager and System Manager

- System Manager disallows IPv6 type of **IP Network Map** while generating Session Manager location.
- System Manager disallows overlapping ranges while generating Session Manager location, which means setting **Controlled by this CM Server** to **Yes**.
- System Manager disallows generating the Session Manager **Location**, when Communication Manager **IP Network Region Name** is blank or if location exists with same name on Session Manager.
- The Communication Manager **IP Network Region** with **Controlled by this CM Server** and corresponding Session Manager **Location** are mapped using correlation ID.

# Chapter 11: Managing backup and restore

## Backup and restore

Use the backup and restore functionality of System Manager to back up and restore the data and configuration files. The data and configuration files for the entire system are kept centrally on System Manager.

 **Note:**

System Manager does not support deployments or upgrades on System Platform. Therefore, for System Manager upgrades by using data migration utility, create a backup of System Manager configuration files and the System Manager database only from the System Manager web console.

During the backup operation, System Manager validates the backup file that you upload, and displays an error if the file type does not match.

You can perform either a backup or a restore operation at a specified time. The restore operation fails if a backup operation is in progress. When a restore operation is in progress, the system skips all backup jobs that you scheduled.

You can restore the data on System Manager that has the same software version and IP address or FQDN as that of System Manager on which you created the backup.

System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

To perform the backup and restore operations, you must map the user to the role with the following permissions:

| Resource type                           | Permissions                   |
|-----------------------------------------|-------------------------------|
| OnDemand                                | add                           |
| All elements of type:SMGR Core Services | backup and restore            |
| All elements of type:alarmoperation     | view and modify               |
| All elements of type:elements           | add, change, delete, and view |

For instructions to create a custom role, see “Adding a custom role”.

 **Note:**

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.



**Related links**

[/emdata/svars/ backup in System Manager](#) on page 839

[Backup failure due to lack of disk space in /swlibrary](#) on page 839

---

## **/emdata/svars/ backup in System Manager**

For the System Manager backup operation, note the following:

- System Manager backup operation supports a maximum of 4GB file size of the `/emdata/svars/` directory. This is approximately 41% of `/emdata` occupancy as displayed in the System Resource Utilization widget on the System Manager web console Home screen.
- If you have 250K users and 4GB of `svars` file size, the backup file size will be of 5GB.

To process the backup in the `/swlibrary` directory, you must have three times of backup file size space.

**Related links**

[Backup and restore](#) on page 838

---

## **Backup failure due to lack of disk space in /swlibrary**

**Condition**

If the backup is not successful due to lack of disk space in `/swlibrary`, check the `/var/log/Avaya/mgmt/pem/pemDebugLog.log` file and search for the below string:

Caused by: `java.io.IOException: No space left on device`

**Solution**

1. Clean up space in `/swlibrary`.

 **Note:**

Do not delete the `wildfly_java_tmp` directory.

2. Move the backup archives, which are located at `/swlibrary/backup/` to remote machine.
3. Delete unused SDM artifacts, such as OVAs and patches that are not required.

To delete SDM artifacts from the System Manager web console, click **Services > Solution Deployment Manager > Software Library Management > Manage Files > Select and Delete files**.

4. Delete any files, such as OVAs for patch binaries copied manually.

**Related links**

[Backup and restore](#) on page 838

---

## Disk space management for System Manager backup

Ensure that sufficient disk space is available before you create a local backup.

The system generates an alarm when the disk space reaches the threshold value. On the System Manager web console, you can configure the disk space and threshold value on the View Profile:SMGR Element Manager page from **Settings > SMGR > SMGR Element Manager**.

When the system runs out of disk space, the system deletes the older backup files to accommodate the new backup files.

For scheduled backups, the system cleans the backup files that local scheduled jobs create every 24 hours. If the number of backup files for each job exceeds 10, the system deletes the older backup files from the file system and removes the corresponding entry from the database.

For remote scheduled backups, the system removes the entries of older backup archive files from the database. However, the system does not delete the backup archive files from the file system.

When a local backup job is running and disk space reaches the maximum limit, the backup job fails. The system displays a message about the insufficient disk space and suggests you to remove older backup files to create additional disk space.

### Related links

[Disk space required for backup](#) on page 850

---

## Backup and restore on System Manager that is configured for Geographic Redundancy

When you create a backup of the System Manager data or restore the data on System Manager that is configured for Geographic Redundancy, you must understand the following facts:

- The secondary System Manager that is in the standby mode does not display the **Backup and Restore** link on the web console.
- You can view the backups that you created on a standalone System Manager only on the web console of that standalone System Manager and after you convert the standalone server to primary System Manager server.
- You can view the backups that you created on a primary System Manager only on the web console of that primary System Manager.
- You can view the backups that you created on a secondary System Manager only on the web console of that secondary System Manager.
- You can restore the backup data from System Manager that is configured for Geographic Redundancy on a standalone System Manager. However, you cannot restore the backup data from a standalone System Manager on System Manager that is configured for Geographic Redundancy.

- You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.
- After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.
- When you enable the Geographic Redundancy replication, the system replicates the backup job that is scheduled on the primary System Manager as the scheduled backup job on the secondary System Manager. The subsequent scheduled backup job runs on both the primary and secondary System Manager separately.

---

## Accessing the Backup and Restore service

### Procedure

On System Manager Web Console, click **Services** > **Backup and Restore**.

#### **Note:**

The secondary System Manager that is in the standby mode does not display the **Backup and Restore** link on the web console.

### Result

The system displays the Backup and Restore page.

### Related links

[Backup and restore](#) on page 838

---

## Viewing list of backup files

### Procedure

On the System Manager web console, click **Services** > **Backup and Restore**.

### Result

The system displays the Backup and Restore page with the list of backup files.

### Related links

[Backup and Restore field descriptions](#) on page 853

---

## Enabling backup encryption

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR > SMGR Element Manager**.
3. On the View Profile:SMGR Element Manager page, click **Edit**.
4. On the Edit Profile:SMGR Element Manager page, in **Backup Encrypted**, type `true`.
5. In **Encrypted Backup Global Password**, type a backup encryption password.
6. Click **Commit**.

---

## Creating a data backup on a local server

### About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

### Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In **File name**, type the backup file that you want to create.
5. **(Optional)** To create encrypted backup using encryption password, do the following:

- a. Clear the **Use Global Backup Encryption Password** check box.

System Manager displays the following fields:

- **Backup Encryption Password**
- **Confirm Backup Encryption Password**

- b. In **Backup Encryption Password**, type the encryption password.
- c. In **Confirm Backup Encryption Password**, retype the encryption password.

You must remember the password to restore the backup.

6. Click **Now**.

If the backup is successful, the Backup and Restore page displays the message: Backup job submitted successfully. Please check the status detail below!!

### Related links

[Backup and restore on System Manager that is configured for Geographic Redundancy](#) on page 840

[Backup field descriptions](#) on page 853

## Creating a data backup on a remote server

### Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup.

System Manager requires password authentication to enable the remote backup servers for successful backup.

### **Note:**

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

### Procedure

1. On the System Manager Web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
  - Perform the following:
    - a. In the **File transfer protocol** field, click **SCP** or **SFTP**.
    - b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
  - Select the **Use Default** check box.

### **Important:**

To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services > Configurations** and navigate to **Settings > SMGR > SMGR Element Manager**.

5. **(Optional)** To create encrypted backup using encryption password, do the following:
  - a. Clear the **Use Global Backup Encryption Password** check box.  
System Manager displays the following fields:
    - **Backup Encryption Password**
    - **Confirm Backup Encryption Password**
  - b. In **Backup Encryption Password**, type the encryption password.

- c. In **Confirm Backup Encryption Password**, retype the encryption password.

You must remember the password to restore the backup.

6. Click **Now**.

If the backup is successful, the Backup and Restore page displays the message: Backup job submitted successfully. Please check the status detail below!!

#### Related links

[Backup and restore on System Manager that is configured for Geographic Redundancy](#) on page 840

[Backup field descriptions](#) on page 853

---

## Scheduling a data backup on a local server

### Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Local**.
4. In the **File name** field, enter the name of the backup file that you want to create.
5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
  - Job name
  - Date and time when the system must run the job
  - Frequency at which the system must run the job
  - Range
7. Click **Commit**.

#### Related links

[Backup field descriptions](#) on page 853

[Schedule Backup field descriptions](#) on page 855

---

## Scheduling a data backup on a remote server

### Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

## About this task

Use this functionality to schedule a data backup on a remote server. If you do not schedule a System Manager backup on a remote server every 7 days, the system generates an alarm.

## Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
  - Specify the SCP server IP, SCP server port, user name, password, and file name in the respective fields.
  - Select the **Use Default** check box.

### Important:

To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services > Configurations** and navigate to **Settings > SMGR > SMGR Element Manager**.

5. Click **Schedule**.
6. On the Schedule Backup page, specify the following details in the appropriate fields:
  - Job name
  - Date and time when the system must run the job
  - Frequency at which the system must run the job
  - Range
7. Click **Commit**.

If you do not schedule a System Manager backup every 7 days, the system generates an alarm.

## Related links

[Backup field descriptions](#) on page 853

[Schedule Backup field descriptions](#) on page 855

---

## Editing a scheduled backup job

To change the backup parameters of a scheduled backup, delete the scheduled backup job and schedule a new backup with the required parameters.

## Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. Click **Pending Jobs**.
3. On the Pending Jobs page, select the backup job.
4. Delete the backup job.

For instructions to delete the scheduled backup job, see [Deleting the scheduled backup job](#).

5. Schedule a new backup job with the changed parameters using one of the following procedures:
  - [Scheduling a data backup on a local server](#).
  - [Scheduling a data backup on a remote server](#).

## Related links

[Scheduling a data backup on a remote server](#) on page 844

[Scheduling a data backup on a local server](#) on page 844

[Deleting the scheduled backup job](#) on page 846

---

# Deleting the scheduled backup job

## Before you begin

Log on to the system as an administrator.

## Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. Click **Pending Jobs**.
3. On the Pending Jobs page, select the backup job that you must delete.
4. Perform one of the following steps:
  - If the backup job that you must delete is currently running, click **More Actions > Stop** to stop the job.
  - If the backup job that you must delete is in the enabled state, click **More Actions > Disable** to disable the job.

For instructions, see [Disabling a job](#) on page 1101.

5. Click **Delete**.
6. On the Delete Confirmation page, click **OK**.

System Manager deletes the backup job from the database.



## Next steps

You can create a new scheduled backup job from **Services > Backup and Restore**.

## Related links

[Editing a scheduled backup job](#) on page 845

---

# Restoring data backup from a local server

## About this task

With Release 8.1.2, you can create and restore encrypted backup after enabling backup encryption.

### Note:

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

## Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Local**.
4. In the **File name** field, type the file name that you must restore.

If the file name does not appear in the list, specify the absolute path to the backup file and the file name that you must restore.

### Note:

System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

5. **(Optional)** To restore encrypted backup using encryption password, do the following:
  - a. Clear the **Use Global Backup Encryption Password** check box.  
System Manager displays the **Backup Encryption Password** field.
  - b. In **Backup Encryption Password**, type the encryption password.
6. Click **Restore**.

On the Restore Confirmation page, the system displays the following message:

The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.

7. Click **Continue**.

The system logs you out of the System Manager web console and then shuts down.

### Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

### Related links

[Backup and restore on System Manager that is configured for Geographic Redundancy](#) on page 840

[Restore field descriptions](#) on page 856

---

## Restoring a backup from a remote server

### About this task

 **Note:**

You cannot restore the backup data on the primary System Manager server when the Geographic Redundancy replication is enabled on System Manager.

To restore the original system at any point of time, you must restore the backup on the same release and the same software patch of that of the original System Manager. For example, if you have created a backup of System Manager Release 8.1 with Release 8.1.1 software patch installed, System Manager on which you restore the backup must run Release 8.1 that has Release 8.1.1 software patch installed.

If the System Manager release on which you restore the backup does not match, the restore operation fails.

### Procedure

1. On the System Manager web console, click **Services > Backup and Restore**.
2. On the Backup and Restore page, click **Restore**.
3. On the Restore page, click **Remote**.
4. **(Optional)** To restore encrypted backup using encryption password, do the following:
  - a. Clear the **Use Global Backup Encryption Password** check box.  
System Manager displays the **Backup Encryption Password** field.
  - b. In **Backup Encryption Password**, type the encryption password.
5. To specify the file name for the restore operation, perform one of the following:
  - Click the **Backup List** tab, and select a file name.

Use this method if the path of the backup file on the remote server is valid, and the credentials used while creating the backup file is unaltered.

- Click the **Parameterized Restore** tab, enter a valid file name, the file transfer protocol, the remote server IP address, remote server port, user name, and the password to access the remote computer in the respective fields.

 **Note:**

System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

- Click the **Parameterized Restore** tab, select the **Use Default** check box.

 **Important:**

To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services > Configurations** and navigate to **Settings > SMGR > SMGR Element Manager**.

6. Click **Restore**.

On the Restore Confirmation page, the system displays the following message:

The Restore operation will terminate all sessions and no services will be available until the operation completes. So, the System Manager console will not be available for approximately 45 minutes but this time may vary based on Database size. Click on Continue to go ahead with the Restore operation or click on Cancel to abort the operation.

7. Click **Continue**.

The system logs you out of the System Manager web console and then shuts down.

## Result

After the restore is complete on System Manager that is configured for Geographic Redundancy, the system automatically restarts with the Geographic Redundancy replication status as disabled.

## Related links

[Backup and restore on System Manager that is configured for Geographic Redundancy](#) on page 840

[Restore field descriptions](#) on page 856

---

# Restoring the backup through the command line interface

## Before you begin

Start an SSH session and provide the correct IP address and the port number.

## About this task

You can restore the data through the command line when the machine is in an unstable state and the system does not display the Web console.

## Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. At the prompt, type `cd $MGMT_HOME/pem/fileRestoreCLIUtility`, and do the following:
  - a. In the `restorecli.properties` file, type the build number of the machine in the **version** field.
  - b. In the properties file, ensure that `fq_backup_file_name` displays the complete path of the backup zip file.
  - c. In the `fileRestoreCLIUtility.properties` file, ensure that `backup_name` points to the backup zip file.
3. Type `sh $MGMT_HOME/pem/fileRestoreCLIUtility/file_restore.sh<full path of fileRestoreCLIUtility><0/1>`.

Where, *0* denotes only the file restore and *1* denotes a full restore.

 **Note:**

System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.

4. Complete the steps on the screen to perform the restore operation successfully.

## Disk space required for backup

Table 8: System Manager backup file size

| Number of users | Database size | Approximate backup file size |        |
|-----------------|---------------|------------------------------|--------|
|                 |               | System Manager               |        |
|                 |               | Local                        | Remote |
| 1k              | 524MB         | 27M                          | 27M    |
| 5k              | 2253MB        | 29M                          | 29M    |
| 25k             | 2774MB        | 34M                          | 34M    |
| 50k             | 4066MB        | 42M                          | 42M    |
| 75k             | 5601MB        | 49M                          | 49M    |

*Table continues...*

| Number of users | Database size | Approximate backup file size |     |
|-----------------|---------------|------------------------------|-----|
|                 |               | System Manager               |     |
| 100k            | 6482MB        | 56M                          | 56M |
| 150k            | 7855MB        | 69M                          | 69M |
| 200k            | 8219MB        | 81M                          | 81M |
| 250k            | 8537MB        | 94M                          | 94M |

---

## Time duration for backup and restore

| Backup and Restore Time Duration |                |                    |
|----------------------------------|----------------|--------------------|
| Number of users                  | System Manager |                    |
|                                  | Backup         | Restore            |
| 1k                               | 57 sec         | 22 min 41 sec      |
| 5k                               | 1 min 15 sec   | 36 min 23 sec      |
| 25k                              | 1 min 46 sec   | 48 min 23 sec      |
| 50k                              | 2 min 03 sec   | 50 min 27 sec      |
| 75k                              | 2 min 32 sec   | 56 min 11 sec      |
| 100k                             | 2 min 54 sec   | 1 hr 4 min 03 sec  |
| 150k                             | 4 min 02 sec   | 1 hr 6 min 52 sec  |
| 200k                             | 4 min 55 sec   | 1 hr 14 min 40 sec |
| 250k                             | 5 min 54 sec   | 1 hr 20 min 40 sec |

---

## Supported ciphers, key exchange algorithms, and mac algorithms

For a successful System Manager remote backup, the remote backup server must support at least one algorithm from each of the following categories:

- Kex algorithms
  - diffie-hellman-group1-sha1
  - diffie-hellman-group-exchange-sha1
  - diffie-hellman-group-exchange-sha256
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384

- ecdh-sha2-nistp521
- Encryption algorithms for Client to Server
  - aes128-ctr
  - 3des-ctr
  - aes192-ctr
  - aes256-ctr
  - 3des-cbc
  - blowfish-cbc
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - arcfour
  - arcfour128
  - arcfour256
- Mac algorithm for Client to Server
  - hmac-sha1
  - hmac-md5
  - hmac-md5-96
  - hmac-sha1-96
  - hmac-sha256
  - hmac-sha2-256
  - hmac-sha256@ssh.com
  - hmac-sha2-256-96
  - hmac-sha512
  - hmac-sha2-512
  - hmac-sha512@ssh.com
  - hmac-sha2-512-96

## Backup and Restore field descriptions

| Name                      | Description                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operation</b>          | The type of operation. The values are: <ul style="list-style-type: none"> <li>• Backup</li> <li>• Restore</li> </ul>                                                                                        |
| <b>File Name</b>          | <ul style="list-style-type: none"> <li>• For the backup operation, the name of the backup file.</li> <li>• For the restore operation, the name of the backup file that was used for the restore.</li> </ul> |
| <b>Path</b>               | <ul style="list-style-type: none"> <li>• For the backup operation, the path of the backup file.</li> <li>• For the restore operation, the path of the backup file that was used for the restore.</li> </ul> |
| <b>Status</b>             | The status of the backup or restore operation. The values are: <ul style="list-style-type: none"> <li>• SUCCESS</li> <li>• FAILED</li> <li>• PLANNED</li> <li>• RUNNING</li> </ul>                          |
| <b>Status Description</b> | The error details of the backup or restore operation that has failed.                                                                                                                                       |
| <b>Operation Time</b>     | The time of the backup or restore operation.                                                                                                                                                                |
| <b>Operation Type</b>     | Defines whether the backup or restore operation is local or remote.                                                                                                                                         |
| <b>User</b>               | The user who performed the operation.                                                                                                                                                                       |

| Button         | Description                                                                      |
|----------------|----------------------------------------------------------------------------------|
| <b>Backup</b>  | Displays the Backup page from where you can back up the System Manager data.     |
| <b>Restore</b> | Displays the Restore page from where you can restore the data to System Manager. |

## Backup field descriptions

| Name        | Description                                                                                                                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b> | The type of computer on which you can back up the application data. The options are: <ul style="list-style-type: none"> <li>• <b>Local:</b> The system backs up the data on a local computer.</li> <li>• <b>Remote:</b> The system backs up the data on a remote computer.</li> </ul> |

The page displays the following fields when you choose to create a backup of System Manager data in a location that is local to the System Manager file system.

| Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b>                             | The file name that identifies the backup.<br><br>System Manager creates a backup file in the home directory of the specified user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Use Global Backup Encryption Password</b> | The option to use the global encryption password for backup.<br><br>To use the <b>Use Global Backup Encryption Password</b> option, enable <b>Backup Encrypted</b> and provide the encryption password on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR &gt; SMGR Element Manager</b> page.<br><br>By default, <b>Use Global Backup Encryption Password</b> is enabled.<br><br>To set a new password for backup, you can deselect the <b>Use Global Backup Encryption Password</b> check box. System Manager displays the following fields:<br><br><ul style="list-style-type: none"> <li>• <b>Backup Encryption Password</b></li> <li>• <b>Confirm Backup Encryption Password</b></li> </ul> |
| <b>Backup Encryption Password</b>            | The password for the encrypted backup.<br><br>The backup encryption password must contain minimum 8 and maximum 16 characters. The password must be a combination of lower case (a-z), upper case (A-Z), numerals (0-9), and special characters (\$@!%*?&).                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Confirm Backup Encryption Password</b>    | The password for the encrypted backup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

The page displays the following fields when you choose to create a backup of the System Manager data on a remote server.

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use Default</b>            | The option to use the default configured values.<br><br>To use the <b>Use Default</b> option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For <b>Use Default</b> , on the SMGR Element Manager page, you can click <b>Services &gt; Configurations</b> and navigate to <b>Settings &gt; SMGR &gt; SMGR Element Manager</b> . |
| <b>File transfer protocol</b> | The protocol that you can use to create the backup. The values are SCP and SFTP.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Remote Server IP</b>       | The IP address of the remote server.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Remote Server Port</b>     | The SSH port of the remote server.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>User Name</b>              | The user name for logging into the remote server.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Password</b>               | The password for logging on to the remote server.                                                                                                                                                                                                                                                                                                                                                                                  |

*Table continues...*



| Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Test Credentials</b>                      | Validates the login credential.<br>The validation gives the connection result with the remote backup server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>File Name</b>                             | The absolute path to the backup file and the file name. For example, <code>home/admin/smgr_backup_filename</code> . You can specify a different path for the backup file on the SMGR Element Manager Container page.<br>To open the SMGR Element Manager Container page, click <b>Services &gt; Configurations</b> and navigate to <b>Settings &gt; SMGR &gt; SMGR Element Manager</b> .                                                                                                                                                                                                                                                                                                 |
| <b>Use Global Backup Encryption Password</b> | The option to use the global encryption password for backup.<br>To use the <b>Use Global Backup Encryption Password</b> option, enable <b>Backup Encrypted</b> and provide the encryption password on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR &gt; SMGR Element Manager</b> page.<br>By default, <b>Use Global Backup Encryption Password</b> is enabled.<br>To set a new password for backup, you can deselect the <b>Use Global Backup Encryption Password</b> check box. System Manager displays the following fields: <ul style="list-style-type: none"> <li>• <b>Backup Encryption Password</b></li> <li>• <b>Confirm Backup Encryption Password</b></li> </ul> |
| <b>Backup Encryption Password</b>            | The password for the encrypted backup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Confirm Backup Encryption Password</b>    | The password for the encrypted backup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Button          | Description                                                                             |
|-----------------|-----------------------------------------------------------------------------------------|
| <b>Now</b>      | Creates a backup of the data in the specified location immediately.                     |
| <b>Schedule</b> | Displays the Schedule Backup page where you can enter the details to schedule a backup. |
| <b>Cancel</b>   | Closes the Backup page and returns to the Backup and Restore page.                      |

## Schedule Backup field descriptions

Use this page to schedule a job for backing up data by specifying the date and time.

### Job Details

| Name            | Description          |
|-----------------|----------------------|
| <b>Job Name</b> | The name of the job. |

## Job Frequency

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Task Time</b>  | The date and time of running the job.                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Recurrence</b> | <p>The settings define whether the execution of the jobs is a recurring activity or a one-time activity. In case of a recurring job, the field also displays the time interval of recurrence. The options are:</p> <ul style="list-style-type: none"> <li>• Execute task one time only.</li> <li>• Tasks are repeated.</li> </ul> <p>The system generates an alarm if you do not schedule a System Manager backup every 7 days.</p> |
| <b>Range</b>      | <p>The settings define the number of recurrences or date after which the job stops to recur. The options are:</p> <ul style="list-style-type: none"> <li>• No End Date</li> <li>• End After occurrences</li> <li>• End By Date</li> </ul>                                                                                                                                                                                           |
| Button            | Description                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Commit</b>     | Schedules the backup job.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Cancel</b>     | Closes the Schedule Backup page and returns to the Backup Restore page.                                                                                                                                                                                                                                                                                                                                                             |

## Restore field descriptions

Use this page to restore the application data from a local or a remote location.

| Name        | Description                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b> | <p>The type of computer from where you restore the application data. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Local</b>. The data is restored from a local machine.</li> <li>• <b>Remote</b>. The data is restored from a remote machine.</li> </ul> |

The page displays the following fields, when you select **Local** as **Type**.

| Name                    | Description                                                                    |
|-------------------------|--------------------------------------------------------------------------------|
| <b>Select File Name</b> | The list of files from where you select the backup file that you must restore. |

*Table continues...*

| Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b>                             | <p>The name of the backup file that you must restore.</p> <p>If the system does not display the file that you must restore, specify the complete path of the backup file.</p> <p> <b>Note:</b></p> <p>System Manager verifies the signature of the backup files and warns if you restore a corrupted or tampered backup file on System Manager.</p>                                                                                                                                                                                                                                                                        |
| <b>Use Global Backup Encryption Password</b> | <p>The option to use the global encryption password for backup.</p> <p>To use the <b>Use Global Backup Encryption Password</b> option, enable <b>Backup Encrypted</b> and provide the encryption password on the <b>Services &gt; Configurations &gt; Settings &gt; SMGR &gt; SMGR Element Manager</b> page.</p> <p>By default, <b>Use Global Backup Encryption Password</b> is enabled.</p> <p>To set a new password for backup, you can deselect the <b>Use Global Backup Encryption Password</b> check box. System Manager displays the following fields:</p> <ul style="list-style-type: none"> <li>• <b>Backup Encryption Password</b></li> <li>• <b>Confirm Backup Encryption Password</b></li> </ul> |
| <b>Backup Encryption Password</b>            | <p>The password for the encrypted backup.</p> <p>The backup encryption password must contain minimum 8 and maximum 16 characters. The password must be a combination of lower case (a-z), upper case (A-Z), numerals (0-9), and special characters (\$@!%*?&amp;).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Confirm Backup Encryption Password</b>    | The password for the encrypted backup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Backup List

The page displays the following fields when you select **Remote** as **Type**.

The **Backup List** tab displays the list of remote backup files that are created using the SFTP or SCP protocol. Select a backup and click the **Parameterized Restore** tab to change the restore details. For example, if the location of a backup file is modified, specify the correct location of the file in the **File Name** field.

## Parameterized Restore

The page displays the following fields when you select **Remote** as **Type**.

| Name                          | Description                                                                       |
|-------------------------------|-----------------------------------------------------------------------------------|
| <b>File Name</b>              | The name and complete path of the backup file that you want to restore.           |
| <b>File transfer protocol</b> | The protocol that you can use to restore the backup. The values are SCP and SFTP. |
| <b>Remote Server IP</b>       | The IP address of the SFTP or SCP server.                                         |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Server Port</b> | The SSH port of the SFTP or SCP server.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>User Name</b>          | The user name for logging in to the SFTP or SCP server.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Password</b>           | Password for logging in to the SFTP or SCP server.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Use Default</b>        | <p>Select this check box to use the default configured values.</p> <p>To use the <b>Use Default</b> option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For <b>Use Default</b>, on the SMGR Element Manager page, you can click <b>Services &gt; Configurations</b> and navigate to <b>Settings &gt; SMGR &gt; SMGR Element Manager</b>.</p> |

| Button         | Description                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------|
| <b>Restore</b> | Restores the data from the specified backup file.                                                     |
| <b>Cancel</b>  | Cancels any operation in progress, closes the Restore page, and displays the Backup and Restore page. |

# Chapter 12: Configuring applications

---

## Managing data retention rules

---

### Data retention rules

You can configure data retention rules to specify the number of days you want the system to retain the following records:

- Logs in Database
- Log files:
  - Application
  - System
- Backup files stored locally on System Manager
- Cleared alarms
- Aged alarms
- Aged Scheduler Completed Jobs

---

### Excluded log files

System Manager does not delete the following logs while executing the **pruneAllLogs.sh** command.

- /var/log/audit/data/
- /var/log/anaconda/
- /var/log/aide/aide.log
- /var/log/Avaya/cs1000/cs1000\_install\_
- /var/log/Avaya/RHEL-07-010010.log
- /var/log/Avaya/GRState.log
- /var/log/Avaya/kernelupdateflag.log

- /var/log/Avaya/VEProfile.log
- /var/log/Avaya/setStaticRoute.out
- /var/log/Avaya/setStaticRoute.log
- /var/log/Avaya/PostDeployLogs/post\_install\_sp.log
- /var/log/Avaya/easg.log
- /var/log/Avaya/patch\_verification.log
- /var/log/Avaya/applyPatch.out
- /var/log/Avaya/SMGR\_Patch.log
- /var/log/Avaya/patchinstallation
- /var/log/Avaya/conferencing\_install.log
- /var/log/Avaya/enableASG.log
- /var/log/Avaya/RestoreSMGR.log
- /var/log/Avaya/backup\_not\_taken.txt
- /var/log/Avaya/dump\_cleanup\_service.log
- /var/log/Avaya/purgeExportFilesLog.log
- /var/log/Avaya/editHost.log
- /var/log/secure
- /var/log/yum.log
- /var/log/wtmp
- /var/log/avaya/common\_os/hardening\_log
- /var/log/ntpCheck.log
- /var/log/setBootPass.log
- /var/log/btmp
- /var/log/dmesg
- /var/log/boot.log
- /var/log/Avaya/OOBM.log
- /var/log/Avaya/smgrUtilityAudit.log
- /var/log/Avaya/logRetention.log
- /var/log/Avaya/SMGRSSP\_Patch.log
- /var/log/Avaya/VTMupdate.log
- /var/log/userShellLog.log

---

## Accessing the Data Retention Rules service

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Data Retention**.

The system displays the Data Retention page with the Rule list.

---

## Modifying data retention rule

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Data Retention**.

The system displays the Data Retention page with the Rule list.

3. From the Rule List section, select a rule.
4. Click **Edit**.

 **Note:**

If you change the **LogPurgeRule** settings, the export delta functionality might get affected as the permanently deleted users login-names in the delta period are identified on the basis of audit logs of permanently deleted users in the system.

5. In the **Retention Interval (Days)** field, modify the value.
6. Click **Update** to save the value.

### Related links

[Data Retention field descriptions](#) on page 862

---

## Applying data retention rule

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Data Retention**.

The system displays the Data Retention page with the Rule list.

3. From the Rule List section, select a rule.
4. Click **Execute** to apply the rule.

When the rule is applied, System Manager display the following message:

Rule successfully applied.

## Data Retention field descriptions

| Name                      | Description                                                                                                                                                                                                                                                                                                                  |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Option button             | The option to select a data retention rule.                                                                                                                                                                                                                                                                                  |
| Rule Name                 | <p>The name of the rule.</p> <p>Rules are:</p> <ul style="list-style-type: none"> <li>• <b>LogPurgeRule</b></li> <li>• <b>CIRDAlarmPurgeRule</b></li> <li>• <b>AgedAlarmPurgeRule</b></li> <li>• <b>AgedSchedulerCompletedJobsPurgeRule</b></li> <li>• <b>LogRetentionRule</b>: This is applicable for log files.</li> </ul> |
| Rule Description          | <p>A brief description about the data retention rule.</p> <p>For <b>LogRetentionRule</b>, the value range is from 1 through 180 days. Default value for number of days to retain log files is 30 days.</p>                                                                                                                   |
| Retention Interval (Days) | The number of days the data is retained.                                                                                                                                                                                                                                                                                     |

| Button  | Description                                   |
|---------|-----------------------------------------------|
| Edit    | Modifies the selected rule.                   |
| Update  | Saves the rule with changes made to the rule. |
| Cancel  | Cancels the editing operation.                |
| Execute | Applies the selected rule.                    |

## logRetention command

The **logRetention** utility displays the currently administered log retention time.

### Syntax

```
logRetention [-a] [-c] [-d] [-h]
```

- a** Displays all log retention time settings.
- c** Displays current log retention time from database.
- d** Displays log retention time set from properties files.
- h,--help** The option to print help options.



---

## updateLogRetention command

The `updateLogRetention.sh` utility manages the log retention time.

### Syntax

```
updateLogRetention.sh [-p] [-v] [maxRetentionTime]
```

- |                         |                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>-p</b>               | The log files do not get pruned.                                                                                     |
| <b>-v</b>               | Verbose mode.                                                                                                        |
| <b>maxRetentionTime</b> | The Maximum Retention Time in days (optional). If the value is not provided, the current administered value is used. |
| <b>-h</b>               | The option to print help options.                                                                                    |

---

## pruneAllLogs command

The `pruneAllLogs.sh` utility manages the deletion of log files.

### Syntax

```
pruneAllLogs.sh [-b] [-t] [-v] [-h] [maxRetentionTime]
```

- |                         |                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>-b</b>               | Deletes the base log files.                                                                                          |
| <b>-t</b>               | Displays the list of log files that are eligible for deletion. Test mode. Does not delete the log files.             |
| <b>-v</b>               | Verbose mode.                                                                                                        |
| <b>-h</b>               | The option to print help options.                                                                                    |
| <b>maxRetentionTime</b> | The Maximum Retention Time in days (optional). If the value is not provided, the current administered value is used. |

# Configuring applications

## Configuration management

Configuration management provides a configuration repository for System Manager services. Configuration management is responsible for storing configuration data, also called as profiles, for System Manager services and notifying the services of configuration changes.

You can view and edit a profile of a service using Configuration management.

### Related links

[View and Edit Profile SMGR field descriptions](#) on page 874

## View Profile: Agent Management field descriptions

| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Alarm aging keep time</b>          | This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Enterprise auto download</b>       | The value in this field specifies whether to enable or disable enterprise auto downloading. The default value is false.<br><br>If the value is set to true, the enterprise downloads the base rules for all registered agents.                                                                                                                                                                   |
| <b>Enterprise customer reference</b>  | The customer reference for the Enterprise. For example, Avaya.<br><br>A value in this field is required only if polling to upstream enterprise is enabled.                                                                                                                                                                                                                                       |
| <b>Enterprise heartbeat interval</b>  | The time in seconds between heartbeats for Enterprise to Enterprise communication.<br><br>A value in this field is required only if polling to upstream enterprise is enabled.                                                                                                                                                                                                                   |
| <b>Enterprise heartbeat threshold</b> | The heartbeat threshold in seconds for the Enterprise.<br><br>A value in this field is required only if polling to upstream enterprise is enabled.                                                                                                                                                                                                                                               |
| <b>Enterprise platform name</b>       | The value in this field specifies a fully-qualified DataTransport address of the host Enterprise.<br><br>For example: The value of this field will be "avaya.com., Enterprise-dtxjbss01", if the OrganizationFQDN value is "avaya.com." and SpiritPlatformQualifier value is "Enterprise-dtxjbss01".<br><br>A value in this field is required only if polling to upstream enterprise is enabled. |

*Table continues...*

| Name                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enterprise tenancy support</b>        | This field is for tenancy support of SAL. This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                            |
| <b>Enterprise upstream platform name</b> | <p>The value specifies a fully-qualified Data Transport address of the upstream enterprise.</p> <p>For example: The value of this field is "avaya.com., Enterprise-dtxapp06", if the Connection.AvayaTest.FQDN value is "avaya.com." and Connection.AvayaTest.PlatformQualifier value is "Enterprise-dtxapp06".</p> <p>A value in this field is required only if polling to upstream enterprise is enabled.</p> |
| <b>Enterprise upstream polling</b>       | <p>The value in this field specifies whether polling upstream enterprise is enabled or not. The default value is false.</p> <p>A false value disables upstream Enterprise polling or Cascading Enterprise.</p>                                                                                                                                                                                                  |
| <b>Inventory aging keep time</b>         | This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Inventory change keep time</b>        | This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Out Of Service delete time</b>        | This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                                                                      |

| Button      | Description                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile: Agent Management page. Use this page to edit the parameters in the Agent Management profile. |
| <b>Done</b> | Closes the View Profile: Agent Management page.                                                                         |

## Configuring IP Office

### Procedure

1. On the System Manager console, click **Services > Configurations**.
2. Click **Settings > IP Office > Configuration**.
3. On the View Profile: Configuration page click **Edit**.
4. Edit the table properties and general properties in the Edit Profile: Configuration page.
5. Click **Commit**.

## IP Office profile field descriptions

| Name                                           | Description                                                                                          |
|------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Maximum Records for Select All in table</b> | The maximum number of records that is used for selection if <b>Select All</b> is used in list pages. |

*Table continues...*

| Name                                           | Description                                           |
|------------------------------------------------|-------------------------------------------------------|
| <b>Maximum Records on single page of table</b> | The maximum number of records displayed in the table. |

## General Properties

| Name                      | Description                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Application Prefix</b> | The name to display as prefix in the Communication System Management job names. The default is IPO. |

| Button        | Description                                                      |
|---------------|------------------------------------------------------------------|
| <b>Edit</b>   | Displays the Edit: Profile page where you can change the values. |
| <b>Done</b>   | Saves the changes.                                               |
| <b>Commit</b> | Saves the changes you make on the Edit: Profile page.            |
| <b>Cancel</b> | Cancels your action and takes you to the View: Profile page.     |

## View Profile: Communication System Management Configuration field descriptions

### Telephony Properties

| Name                                                          | Description                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Clean-up Old Backup Announcement Files interval (Days)</b> | The time between every clean up of the backed up announcement files. The default value is 30 days.                                                                                                                                                                                          |
| <b>Pre-populate extension values in User Management</b>       | Enter <code>true</code> in this field if you want the system to pre populate the extension value in User Management, Communication Manager communication profile.                                                                                                                           |
| <b>Endpoint Migration Job History Retention in Days</b>       | The number of days to retain the endpoint migration job history data.<br>The number of days for retaining the endpoint migration job history data is from 1 through 60 days. By default, the number of days for the <b>endpoint_migration_job_history_retention_days</b> field are 30 days. |
| <b>Incremental sync interval (Hours)</b>                      | The time between every incremental synchronization. By default, the value for the <b>incremental_sync_interval_in_hours</b> field is 24 hours.                                                                                                                                              |
| <b>Maximum Records for select All in table</b>                | The maximum number of records that is used for selection if <b>Select All</b> is used in list pages.                                                                                                                                                                                        |
| <b>Maximum Records on single page of table</b>                | The maximum number of records displayed in the table.                                                                                                                                                                                                                                       |

## General Properties

| Name                      | Description                                                                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application Prefix</b> | The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names.           |
| <b>Button</b>             | <b>Description</b>                                                                                                                                |
| <b>Edit</b>               | Click to open the Edit Profile:Communication System Management Configuration page. Use this page to edit the parameters in the Scheduler profile. |
| <b>Done</b>               | Click to close the Edit Profile:Communication System Management Configuration page.                                                               |

## Edit Profile: Communication System Management Configuration field descriptions

Use this page to edit the parameters in the Communication System Management Configuration profile.

### Telephony Properties

| Name                                                          | Description                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Clean-up Old Backup Announcement Files interval (Days)</b> | The time between every clean up of the backed up announcement files. The default value is 30 days.                                                                                                                                                                                          |
| <b>Pre-populate extension values in User Management</b>       | Enter <code>true</code> in this field if you want the system to pre populate the extension value in User Management, Communication Manager communication profile.                                                                                                                           |
| <b>Endpoint Migration Job History Retention in Days</b>       | The number of days to retain the endpoint migration job history data.<br>The number of days for retaining the endpoint migration job history data is from 1 through 60 days. By default, the number of days for the <b>endpoint_migration_job_history_retention_days</b> field are 30 days. |
| <b>Incremental sync interval (Hours)</b>                      | The time between every incremental synchronization. By default, the value for the <b>incremental_sync_interval_in_hours</b> field is 24 hours.                                                                                                                                              |
| <b>Maximum Records for select All in table</b>                | The maximum number of records that is used for selection if <b>Select All</b> is used in list pages.                                                                                                                                                                                        |
| <b>Maximum Records on single page of table</b>                | The maximum number of records displayed in the table.                                                                                                                                                                                                                                       |

### General Properties

| Name                      | Description                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application Prefix</b> | The default value in this field is CSM. This application prefix appears as the prefix in the Communication System Management job names. |

| Button        | Description                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                                                                     |
| <b>Cancel</b> | Cancels the edit profile operation and returns to the Edit Profile:Communication System Management Configuration page. |

## View Profile: Event processor field descriptions

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>EP mechanism class name 1</b> | This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>EP mechanism XSD type</b>     | <p>The value in this field specifies event processor uses a set of XML rule configuration files to describe the rules to be used to process events.</p> <p>The event processor uses a different processing mechanisms as indicated by the type of rule listed in a rule configuration file.</p> <p>A mapping between the XSD types describes rules and the java classes used to implement the rule processing mechanisms is required.</p> <p>For every concrete XSDType used to implement a processingMechanismConfigurationType, the event processor must have a mapping to an available java class.</p> <p>The XSDType: Java Class mappings are done by creating sets of matching pair entries in the &lt;Attributes &gt; element below:</p> <ol style="list-style-type: none"> <li>1. The first is a &lt;string&gt; element with a name of "EPMechanismXSDType.N" where N is a positive integer. The value of the entry indicates the full URI of the type name, including the namespace.</li> <li>2. The second is an &lt;string&gt; element named "EPMechanismClassName.N" where N matches the appropriate EPMechanismXSDType entry. The Event Processor will incrementally search for XSDType-&gt;Class mappings, beginning with an "N" of 1 and working incrementally positive until it can't find a type or class for the current N.&lt;/string&gt;&lt;/string &gt;&lt;/Attributes&gt;</li> </ol> |
| <b>EP transport address</b>      | This field is not used for System Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Button      | Description                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile: Event processor page. Use this page to edit the parameters in the Event processor profile. |
| <b>Done</b> | Closes the View Profile: Event processor page.                                                                        |

## View Profile:Configuration field descriptions

### Reports cleanup properties

| Name                                               | Description                                                                                                      |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Reports periodic Cleanup Interval (in days)</b> | The interval in days when the system performs the cleanup. By default, the system deletes reports after 60 days. |

### Reports Output Directory

| Name                                 | Description                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Reports Output Directory</b>      | The name of the directory where the system saves the reports. The default location is /opt/Avaya/reports_data.              |
| <b>Reports Output Directory Size</b> | The maximum size of the output directory that is allocated on System Manager to save the reports. The maximum size is 1 GB. |

### Reports Alarm Properties

| Name                                                                            | Description                                                                                                      |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Raise critical alarm in case Reports Output Directory fills (in percent)</b> | The percentage of space in the output directory when the system must raise a critical alarm. The default is 95%. |
| <b>Raise major alarm in case Reports Output Directory fills (in percent)</b>    | The percentage of space in the output directory when the system must raise a major alarm. The default is 85%.    |
| <b>Raise minor alarm in case Reports Output Directory fills (in percent)</b>    | The percentage of space in the output directory when the system must raise a minor alarm. The default is 70%.    |

| Button      | Description                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the View Profile:Configuration page. Use the View Profile:Configuration page to configure the <b>Configuration</b> parameter. |
| <b>Done</b> | Closes the View Profile:Configuration page.                                                                                            |

## View profile:Inventory field descriptions

To navigate to this page, click **Services > Configurations > Settings > Inventory > Configuration**.

## General Properties

| Name                                                                           | Description                                                                                        |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Maximum number of threads for the step Collecting Inventory Information</b> | The maximum number of Java threads created and used for the step Collecting Inventory Information. |
| <b>Maximum number of threads for the step Probing Network Elements</b>         | The maximum number of Java threads created and used for the step Probing Network Elements.         |
| <b>Maximum Records on single page of table</b>                                 | The total number of rows displayed in a table.                                                     |

| Button      | Description                                                           |
|-------------|-----------------------------------------------------------------------|
| <b>Edit</b> | Returns to the Edit Profile: Configuration page in <b>Inventory</b> . |
| <b>Done</b> | Closes the View Profile: Configuration page.                          |

---

## Edit Profile:Inventory field descriptions

### General Properties

| Name                                                                           | Description                                                                                        |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>Maximum number of threads for the step Collecting Inventory Information</b> | The maximum number of Java threads created and used for the step Collecting Inventory Information. |
| <b>Maximum number of threads for the step Probing Network Elements</b>         | The maximum number of Java threads created and used for the step Probing Network Elements.         |
| <b>Maximum Records on single page of table</b>                                 | The total number of rows displayed in a table.                                                     |

| Button        | Description                                                       |
|---------------|-------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes and closes the Edit Profile: Configuration page |
| <b>Cancel</b> | Cancels your action and returns to the previous page.             |



## View and Edit Profile Messaging field descriptions

### Telephony Properties

| Name                                           | Description                                                                                                                             |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum Records for select All in table</b> | The maximum number of records that the system selects if <b>Select All</b> is used in list pages.<br>The default value is <b>1000</b> . |
| <b>Maximum Records on single page of table</b> | The maximum number of records that the system displays in the table.<br>The default value is <b>200</b> .                               |

### General Properties

| Name                                                                                                                                        | Description                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Append Mailbox Number to Email Handle when adding the Avaya Aura Messaging subscriber</b>                                                | When adding Avaya Aura® Messaging Subscriber the system appends the mailbox number to the email.<br>The default value is <b>false</b> .  |
| <b>Application Prefix</b>                                                                                                                   | The text that the system prefixes to the Messaging System job names.<br>The default value is <b>MM</b> .                                 |
| <b>Refresh Subscriber data from Messaging during edit/view</b>                                                                              | Refreshes the subscriber data from Messaging Server on edit/view.<br>The default value is <b>false</b> .                                 |
| <b>Update Email Handle, Common Name and ASCII version of name when changing the Avaya Aura Messaging subscriber First, Last Name values</b> | Updates Email Handle, Common Name and ASCII version of name fields on first or last name changes.<br>The default value is <b>false</b> . |

### View Profile: Configuration buttons

| Button      | Description                                                                     |
|-------------|---------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the View Profile: Messaging Configuration page to edit the properties. |
| <b>Done</b> | Returns to the previous page.                                                   |

### Edit Profile: Configuration buttons

| Button        | Description                                                          |
|---------------|----------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes on the Edit Profile: Messaging Configuration page. |
| <b>Cancel</b> | Cancels the changes and displays the previous page.                  |

## View Profile: Data Transport Config field descriptions

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Connection Avaya production FQDN</b>               | The value is a fully qualified domain name of the target Enterprise for a connection. This may identify a customer, Business Partner or Avaya itself. For example, avaya.com, company.com                                                                                                                                                                                                                                                        |
| <b>Connection Avaya production keyAlias</b>           | The value specifies the alias of a key in the keyStore to be used for client authentication in HTTPS sessions when communicating with an upstream server. Typically used when Avaya is the upstream server.<br><br>This is an optional field.                                                                                                                                                                                                    |
| <b>Connection Avaya production platform qualifier</b> | The value is a logical name for the target enterprise, that applies irrespective of primary or backup.<br><br>The primary and backup are a part of the same organization. Components use this name to address the Enterprise Server pair.<br><br>This name must match the name that the Enterprise Servers have assigned to themselves locally or else the connection is rejected.                                                               |
| <b>Connection Avaya production primary URL</b>        | The value is a primary URL of the platform                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Connection Avaya production useProxy</b>           | The value specifies whether to use proxies for this platform or not. The values are true or false.                                                                                                                                                                                                                                                                                                                                               |
| <b>Connection set</b>                                 | The set of connections that this SAL data transport will open.<br><br>Each connection must have PlatformName, TargetFQDN, and PrimaryURL elements. Connections can optionally also have BackupURL elements.                                                                                                                                                                                                                                      |
| <b>Https session timeout</b>                          | The value specifies the maximum duration of HTTPS authentication sessions before they need to be re-negotiated.                                                                                                                                                                                                                                                                                                                                  |
| <b>Max message exchange size</b>                      | The value specifies maximum size of the messages data transport attempts to send or receive in one bundle.<br><br>The following are the units of size: <ul style="list-style-type: none"> <li>• B for bytes</li> <li>• M for megabytes</li> <li>• k for kilobytes</li> </ul> <p> <b>Note:</b><br/>Do not change the default value unless there is a need.</p> |

*Table continues...*

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max queue memory</b>          | <p>The value specifies the maximum amount of memory on disk that the queue can occupy.</p> <p>The following are the units of memory:</p> <ul style="list-style-type: none"> <li>• B for bytes</li> <li>• M for megabytes</li> <li>• k for kilobytes</li> </ul> <p> <b>Note:</b></p> <p>Do not change the default value unless there is a need.</p>                                                                                                                                                                                                   |
| <b>Max send transaction time</b> | <p>The value specifies the maximum amount of time spent in a transaction when trying to send upstream.</p> <p> <b>Note:</b></p> <p>Do not change the default value unless there is a need.</p>                                                                                                                                                                                                                                                                                                                                                       |
| <b>Organization FQDN</b>         | The value specifies a fully qualified domain name that uniquely identifies the business organization that the SAL Platform resides in.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Polling interval</b>          | <p>The time between polling for messages from each enterprise platform. Specify 0 to turn polling off.</p> <p>The following are the units:</p> <ul style="list-style-type: none"> <li>• h for Hours</li> <li>• m for Minutes</li> </ul> <p>The Agent polls because there is no way to connect directly from Avaya to the customer. Connections may only be initiated from the customer side. A component in the Enterprise can just send a message. The message is queued until either a message or a polling request is received from the destination Agent and the queued message is sent back to the Agent in the HTTPS reply.</p> |
| <b>Proxy address</b>             | The domain name or IP address of the proxy to use.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Proxy password</b>            | The password to use with the proxy. They are stored in a plain text.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Proxy port</b>                | The port of the proxy server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Proxy type</b>                | The type of proxy based on whether the proxy supports HTTP or SOCKS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Proxy use authentication</b>  | <p>The value specifies whether an authentication is required to access the proxy server.</p> <p>The values are true and false. If the value is true, an authentication is required to access the server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Proxy user</b>                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table continues...

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Server status reset interval</b> | <p>The time between the server marking an URL as unreachable and reattempting to connect to that URL.</p> <p>The following are the units of time:</p> <ul style="list-style-type: none"> <li>• h for hours</li> <li>• m for minutes</li> <li>• s for seconds</li> </ul>                                                                                                         |
| <b>SAL platform qualifier</b>       | <p>A logical name for the target Enterprise, that applies irrespective of primary or backup. Implicitly, the primary and backup are a part of the same organization. Components use this name to address the Enterprise Server pair. This name must match the name that the Enterprise Servers have assigned to themselves locally or else the connection will be rejected.</p> |

| Button      | Description                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile: Data Transport Config page. Use this page to edit the parameters in the Data Transport Configuration profile. |
| <b>Done</b> | Closes the View Profile: Data Transport Config page.                                                                                     |

---

## View Profile: Data Transport Static Config field descriptions

Do not change any values in the fields displayed on this page. Any change is likely to break the SAL Agent application.

---

## View and Edit Profile SMGR field descriptions

### Key Management Properties

| Name                                                          | Description                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Number of days before administrator should be notified</b> | <p>The number of days before the key expiry when the administrator must be notified.</p> <p>The default is 21.</p>                                                                                                                                                                                                 |
| <b>Notify administrator about asymmetric keys expiration</b>  | <p>The status of the asymmetric keys expiration notification to the administrator. The options are:</p> <ul style="list-style-type: none"> <li>• <code>true</code>: To enable the notifications.</li> <li>• <code>false</code>: To disable the notifications.</li> </ul> <p>The default is <code>false</code>.</p> |

## Database Properties

| Name                    | Description                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------|
| <b>Connection URL</b>   | The connection URL of the database.                                                             |
| <b>Host Name</b>        | The host name of the database.                                                                  |
| <b>JDBC Drive Class</b> | The JDBC drive class for the database.                                                          |
| <b>Password</b>         | The password for logging into the database.                                                     |
| <b>Confirm Password</b> | The database login password that you retype.<br>This option is available only in the Edit mode. |
| <b>Port Number</b>      | The port number of the database.                                                                |
| <b>User Name</b>        | The user name for logging into the database.                                                    |
| <b>Vendor Name</b>      | The vendor name of the database.                                                                |

## Password Policy for Programmatic Accounts

| Name                                                  | Description                                                                                                                                                                                                                                      |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disallow repeated and/or sequential characters</b> | The options are: <ul style="list-style-type: none"> <li>• <b>true</b>: Repeated and sequential characters are not allowed.</li> <li>• <b>false</b>: Repeated and sequential characters are allowed.</li> </ul> By default, this is <b>true</b> . |
| <b>Minimum total length</b>                           | The minimum number of characters that you must use in the password. The valid values are from 1 through 32. The default value is 32.                                                                                                             |
| <b>Minimum number of lower case character(s)</b>      | The minimum number of lowercase characters that you must use in the password. The default value is 0.                                                                                                                                            |
| <b>Minimum number of numeric character(s)</b>         | The minimum number of numeric characters that you must use in the password. The default value is 0.                                                                                                                                              |
| <b>Minimum number of special character(s)</b>         | The minimum number of special characters that you must use in the password. The default value is 0.                                                                                                                                              |
| <b>Minimum number of upper case character(s)</b>      | The minimum number of uppercase characters that you must use in the password. The default value is 0.                                                                                                                                            |
| <b>Previous password(s) blocked</b>                   | The number of recent passwords that you cannot use. The valid values are from 0 through 24. The default value is 24.<br><br>The 0 value means that System Manager does not check for the previous passwords.                                     |

## Multi Tenancy Properties

| Name                        | Description                                                                                                                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Multi Tenancy Status</b> | <p>The status of the Multi Tenancy feature on the system. The options are:</p> <ul style="list-style-type: none"> <li>• <code>true</code>: To enable the feature.</li> <li>• <code>false</code>: To disable the feature.</li> </ul> <p>The default is <code>false</code>.</p> |

## Self Provisioning Properties

| Name                            | Description                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Self Provisioning Status</b> | <p>The option for the end user to change the H323 and SIP passwords. The options are:</p> <ul style="list-style-type: none"> <li>• <code>true</code>: To enable self provisioning.</li> <li>• <code>false</code>: To disable self provisioning.</li> </ul> |

## System Manager Properties

| Name                 | Description                                                                     |
|----------------------|---------------------------------------------------------------------------------|
| <b>Build Version</b> | <p>The build version of System Manager.</p> <p>This field cannot be edited.</p> |

## Auto Transliteration Properties

| Name                             | Description                                                                                                                                                                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto Transliteration Flag</b> | <p>The status of the auto transliteration feature. The options are:</p> <ul style="list-style-type: none"> <li>• <code>true</code>: To enable transliteration.</li> <li>• <code>false</code>: To disable transliteration.</li> </ul> <p>The default is <code>true</code>.</p> |

## Audit Configuration Properties

| Name                                                                 | Description                                                                                                                    |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Number of failed login attempts to indicate a security threat</b> | <p>The number of failed login attempts after which a security threat is indicated.</p> <p>The default is 5 login attempts.</p> |

## Email Configuration Properties

| Name                               | Description                                                                                                                                                                                                                                                              |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable email notification</b>   | The status of the email notifications feature. The options are: <ul style="list-style-type: none"> <li>• <code>true</code>: To enable email notifications.</li> <li>• <code>false</code>: To disable email notifications.</li> </ul> The default is <code>false</code> . |
| <b>From Email Address</b>          | The email ID that the system uses to send the email.                                                                                                                                                                                                                     |
| <b>From Email Password</b>         | The email password that the system uses for authentication before sending the email.                                                                                                                                                                                     |
| <b>Confirm From Email Password</b> | The email authentication password that you retype.<br>This option is available only in the Edit mode.                                                                                                                                                                    |
| <b>Email Host</b>                  | The URL for the email server.                                                                                                                                                                                                                                            |
| <b>Email Host Port</b>             | The port for the email server. The default port is 25.                                                                                                                                                                                                                   |

## View Profile:Alarming UI field descriptions

Use this page to view the parameters in the Alarming profile.

### Color Codes

| Name                 | Description                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Cleared</b>       | The color code for cleared alarms.                                                                           |
| <b>Critical</b>      | The color code for critical alarms.                                                                          |
| <b>Indeterminate</b> | The color code for the indeterminate alarms.<br>You can change the values to specify a different color code. |
| <b>Major</b>         | The color code for the major alarms.                                                                         |
| <b>Minor</b>         | The color code for the minor alarms.<br>You can change the values to specify a different color code.         |
| <b>Warning</b>       | The color code for the warning alarms.<br>You can change the values to specify a different color code.       |

### Auto Refresh

| Name                            | Description                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Time Interval (millisec)</b> | The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page. |

| Button      | Description                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile:Alarming UI page. Use this page to edit the parameters in the Alarming Profile. |
| <b>Done</b> | Closes the View Profile:Alarming UI page.                                                                 |

## Edit Profile:Alarming UI field descriptions

Use this page to edit the parameters in the Alarming profile.

### Color Codes

| Name                 | Description                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Cleared</b>       | The color code for alarms that are cleared.                                                                  |
| <b>Critical</b>      | The color code for critical alarms.                                                                          |
| <b>Indeterminate</b> | The color code for the indeterminate alarms.<br>You can change the values to specify a different color code. |
| <b>Major</b>         | The color code for the major alarms.                                                                         |
| <b>Minor</b>         | The color code for the minor alarms.<br>You can change the values to specify a different color code.         |
| <b>Warning</b>       | The color code for the warning alarms.<br>You can change the values to specify a different color code.       |

### Auto Refresh

| Name                            | Description                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Time Interval (millisec)</b> | The time interval in milliseconds after which the Alarming module refreshes the alarms on the Alarming page. |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                                   |
| <b>Cancel</b> | Cancels the edit profile operation and returns to the View Profile:Alarming UI page. |

## View Profile:Common Console field descriptions

### Note:

For the changes to be effective, log out and log on again to the system.



| Name                                                                              | Description                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max No of tabs that you can open on landing page</b>                           | The maximum number of tabs that you can open from the Home page. The default is 5.<br><br>If you set the number to more than 5, for example 7 and open more than 7 tabs, the system displays You have exceeded the maximum numbers of tabs. Close any one of the tabs to open a new tab. |
| <b>Maximum number of user preferences that can be saved and seen on dashboard</b> | The maximum number of user preferences that you can save and view on the Home page. You can set a value between 10 and 20. The default is 15.                                                                                                                                            |
| <b>Number of rows</b>                                                             | Number of rows that you want the system to display in a table. The range of rows that you can set is 15 through 100. The default is 15.                                                                                                                                                  |
| <b>Max No of Records Selectable (Table)</b>                                       | The maximum number of records that you can select at a time from a table.                                                                                                                                                                                                                |

| Button      | Description                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile: Common Console page where you can edit the common console profile parameters. |
| <b>Done</b> | Closes the View Profile: Common Console page.                                                            |

## Edit Profile:Common Console field descriptions

 **Note:**

For the changes to be effective, log out from the system and log on again.

| Name                                                                              | Description                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max No of tabs that you can open on landing page</b>                           | The maximum number of tabs that you can open from the Home page. The default is 5.<br><br>If you set the number to more than 5, for example 7 and open more than 7 tabs, the system displays You have exceeded the maximum numbers of tabs. Close any one of the tabs to open a new tab. |
| <b>Maximum number of user preferences that can be saved and seen on dashboard</b> | The maximum number of user preferences that you can save and view on the Home page. You can set a value between 10 and 20. The default is 15.                                                                                                                                            |
| <b>Number of rows</b>                                                             | Number of rows that you want the system to display in a table. The range of rows that you can set is 15 through 100. The default is 15.                                                                                                                                                  |
| <b>Max No of Records Selectable (Table)</b>                                       | The maximum number of records that you can select at a time from a table.                                                                                                                                                                                                                |

| Button        | Description                         |
|---------------|-------------------------------------|
| <b>Commit</b> | Saves the changes to the database.  |
| <b>Cancel</b> | Cancels the edit profile operation. |

---

## View Profile:GracefulShutdown field descriptions

| Name                             | Description                                                                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Grace Period (In Minutes)</b> | The time in minutes within which the active users must finish their operations before the administrator shuts down System Manager.<br><br>The default value for the grace period before shutting down System Manager is 10 minutes. |

| Button       | Description                                                                            |
|--------------|----------------------------------------------------------------------------------------|
| <b>Edit</b>  | Displays the Edit Profile:GracefulShutdown page where you can change the grace period. |
| <b>Close</b> | Closes the View Profile:GracefulShutdown page.                                         |

---

## Edit Profile:GracefulShutdown field descriptions

| Name                             | Description                                                                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Grace Period (In Minutes)</b> | The time in minutes within which the active users must finish their operations before the administrator shuts down System Manager.<br><br>The default value for the grace period before shutting down System Manager is 10 minutes. |

| Button        | Description                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes that you made on the Edit Profile:Shutdown page.                                                                  |
| <b>Cancel</b> | Cancels the changes that you made on the Edit Profile:GracefulShutdown page, and returns to the View Profile:GracefulShutdown page. |

---

## View Profile:HealthMonitor field descriptions

### HealthMonitor Configuration Parameters

| Name                          | Description                                                                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>HealthMonitor interval</b> | The time interval, in seconds, within which the Health Monitoring service polls for the information on the system status. |

*Table continues...*

| Name                                | Description                                                                                                   |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>HealthMonitor Retention Days</b> | The number of days the system retains the Health Monitoring data.                                             |
| <b>HealthMonitor Retries</b>        | The number of successive attempts that the Health Monitoring service makes before the system raises an alarm. |

| Button      | Description                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile:HealthMonitor page. Use the Edit Profile:HealthMonitor page to configure the HealthMonitor parameters. |
| <b>Done</b> | Closes the View Profile:HealthMonitor page.                                                                                      |

### Related links

[Edit Profile:HealthMonitor field descriptions](#) on page 881

## Edit Profile:HealthMonitor field descriptions

Use this page to edit the Health Monitor parameters.

### Note:

Click **Edit** to open the Edit Profile:HealthMonitor page.

### HealthMonitor Configuration Parameters

| Name                                | Description                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>HealthMonitor interval</b>       | The time interval, in seconds, within which the Health Monitoring service polls for the information on the system status. |
| <b>HealthMonitor Retention Days</b> | The number of days the system retains the Health Monitoring data.                                                         |
| <b>HealthMonitor Retries</b>        | The number of successive attempts that the Health Monitoring service makes before the system raises an alarm.             |

| Button         | Description                                                                            |
|----------------|----------------------------------------------------------------------------------------|
| <b>Commits</b> | Saves the changes you make on the View Profile:HealthMonitor page.                     |
| <b>Cancels</b> | Cancels the edit profile operation and returns to the View Profile:HealthMonitor page. |

### Related links

[View Profile:HealthMonitor field descriptions](#) on page 880

## View Profile:Licenses field descriptions

| Name                                               | Description                                                                                                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WebLM Usages<br/>UsageCount</b>                 | This count represents the number of usage reports the server must maintain and display for each WebLM server.                                                           |
| <b>WebLM LicenseAllocation<br/>Backup FileSize</b> | This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid. |

| Button      | Description                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile:Licenses (WebLM) page. Use this page to edit the parameters in the WebLM profile. |
| <b>Done</b> | Closes the View Profile:Licenses (WebLM) page.                                                              |

## Edit Profile:Licenses field descriptions

| Name                                               | Description                                                                                                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WebLM Usages<br/>UsageCount</b>                 | This count represents the number of usage reports the server must maintain and display for each WebLM server.                                                           |
| <b>WebLM LicenseAllocation<br/>Backup FileSize</b> | This property specifies the size of the license allocation backup file in MB. Allocate an integer to this property like 1 or 10. A decimal value like 1.5 is not valid. |

| Button        | Description                                                                               |
|---------------|-------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                                        |
| <b>Cancel</b> | Cancels the edit profile operation and returns to the View Profile:Licenses (WebLM) page. |

## View Profile:Logging UI field descriptions

### Log Severity Levels

| Name            | Description                                                                            |
|-----------------|----------------------------------------------------------------------------------------|
| <b>Alert</b>    | The color code for the log messages that are logged under the Alert severity level.    |
| <b>Critical</b> | The color code for the log messages that are logged under the Critical severity level. |
| <b>Debug</b>    | The color code for the log messages that are logged under the Debug severity level.    |

*Table continues...*

| Name                 | Description                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------|
| <b>Emergency</b>     | The color code for the log messages that are logged under the Emergency severity level.     |
| <b>Error</b>         | The color code for the log messages that are logged under the Error severity level.         |
| <b>Informational</b> | The color code for the log messages that are logged under the Informational severity level. |
| <b>Notice</b>        | The color code for the log messages that are logged under the Notice severity level.        |
| <b>Warning</b>       | The color code for the log messages that are logged under the Notice severity level.        |

### Auto Refresh

| Name                           | Description                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Time Interval(millisec)</b> | The time interval in milliseconds after which the log messages are auto refreshed on the Logging page . |

| Button      | Description                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Profile:Logging page. Use this page to edit the parameters in the Logging profile. |
| <b>Done</b> | Closes the View Profile:Logging page.                                                                |

## Edit Profile:Logging UI field descriptions

### Log Severity Levels

| Name                 | Description                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------|
| <b>Alert</b>         | The color code for the log messages that are logged under the Alert severity level.         |
| <b>Critical</b>      | The color code for the log messages that are logged under the Critical severity level.      |
| <b>Debug</b>         | The color code for the log messages that are logged under the Debug security level.         |
| <b>Emergency</b>     | The color code for the log messages that are logged under the Emergency severity level.     |
| <b>Error</b>         | The color code for the log messages that are logged under the Error severity level.         |
| <b>Informational</b> | The color code for the log messages that are logged under the Informational severity level. |
| <b>Notice</b>        | The color code for the log messages that are logged under the Notice severity level.        |

*Table continues...*

| Name           | Description                                                                          |
|----------------|--------------------------------------------------------------------------------------|
| <b>Warning</b> | The color code for the log messages that are logged under the Notice severity level. |

### Auto Refresh

| Name                              | Description                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Time Interval(millisecond)</b> | The time interval in milliseconds after which the log messages are auto refreshed on the Logging page. |

| Button        | Description                                                                      |
|---------------|----------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                               |
| <b>Cancel</b> | Cancels the edit profile operation and returns to the View Profile:Logging page. |

## View Profile:Logging Service field descriptions

Use this page to view the parameters and their corresponding values that specify the default settings for log harvesting service.

| Name                                                                | Description                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max time interval to wait</b>                                    | The maximum time interval for which the system waits between a request and a response for harvesting a log file from a remote System Manager computer. You can specify a time interval between 1800000 milliseconds to maximum value of 7200000 milliseconds. The default value is 10800000 milliseconds. |
| <b>Directory path for harvested files</b>                           | The directory where all the harvested files are stored. The default path is <code>/var/log/Avaya/mgmt/downloads</code> .                                                                                                                                                                                  |
| <b>No. of Lines/Page(All harvested archives will be re-indexed)</b> | The maximum number of lines that you can view on the log browser page for a harvested log file.                                                                                                                                                                                                           |
| <b>Maximum allowed size of harvest directory (In GB)</b>            | The maximum size of the harvested files directory. The value of minimum size of the harvested directory is 1 GB and maximum size can be 10 GB.                                                                                                                                                            |
| <b>No. of files for File rotation</b>                               | The maximum number of harvested files that the system can store before the oldest file is overwritten by the new harvested file. You can set 10 as minimum number of files and 9999999 as maximum number of files.                                                                                        |

| Button      | Description                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Logging Service Profile page. Use this page to edit the values of the log harvesting parameters. |
| <b>Done</b> | Closes the View Logging Service Profile page.                                                                      |

## Edit Profile:Logging Service field descriptions

Use this page to modify the value of parameters that define settings for log harvesting.

| Name                                                                | Description                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Max time interval to wait</b>                                    | The maximum time interval for which the system waits between a request and a response for harvesting a log file from a remote System Manager computer. You can specify a time interval between 1800000 milliseconds to maximum value of 7200000 milliseconds. The default value is 10800000 milliseconds. |
| <b>Directory path for harvested files</b>                           | The directory where all the harvested files are stored. The default path is <code>/var/log/Avaya/mgmt/downloads</code> .                                                                                                                                                                                  |
| <b>No. of Lines/Page(All harvested archives will be re-indexed)</b> | The maximum number of lines that you can view on the log browser page for a harvested log file.                                                                                                                                                                                                           |
| <b>Maximum allowed size of harvest directory (In GB)</b>            | The maximum size of the harvested files directory. The value of minimum size of the harvested directory is 1 GB and maximum size can be 10 GB.                                                                                                                                                            |
| <b>No. of files for File rotation</b>                               | The maximum number of harvested files that the system can store before the oldest file is overwritten by the new harvested file. You can set 10 as minimum number of files and 9999999 as maximum number of files.                                                                                        |

| Button        | Description                                                                              |
|---------------|------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                                       |
| <b>Cancel</b> | Cancels the edit profile operation and returns to the View Profile:Logging Service page. |

## View and Edit Profile: SMGR Element Manager field descriptions

| Name                          | Description                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Backup Directory</b>       | <p>The name of the directory on the database server where Element Manager creates backup archives.</p> <p>The default directory is <code>swlibrary/backup</code>.</p> <p> <b>Note:</b></p> <p>The database user must have write privileges on this directory.</p> |
| <b>Backup Encrypted</b>       | <p>The option to enable or disable backup encryption. The options are:</p> <ul style="list-style-type: none"> <li>• <code>true</code></li> <li>• <code>false</code></li> </ul>                                                                                                                                                                       |
| <b>Backup Global Password</b> | The global password for the encrypted backup.                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Confirm Backup Global Password</b>            | The global password for the encrypted backup that you retype to confirm.<br>This field is only available in the Edit mode.                                                                                                                                                                                                                                                                                                      |
| <b>Database Utilities Path</b>                   | The name of the directory on the database server that contains the PostgreSQL backup and restore utilities.<br><br> <b>Note:</b><br>The database user must have execute permissions on these utilities.                                                                                                                                        |
| <b>Database Type</b>                             | The type of database. For example, Oracle, Postgres.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Database server</b>                           | The hostname of the database server.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Database Port</b>                             | The port number for the database server.                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Database SCP Port</b>                         | The port on the database server on which the SSH server is running.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Disk Space Allocated (GB)</b>                 | The disk space allocated for backup archives.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Disk Space Threshold (%)</b>                  | The percentage of the <b>diskSpaceAllocated</b> property. When this percentage is reached, the system generates an alarm. For example, if the <b>diskSpaceAllocated</b> is 100 MB and <b>diskSpaceThreshold</b> is 90 percent, the system generates an alarm when the disk space occupied by the backup archives reaches 90 MB.                                                                                                 |
| <b>Job Interface URL</b>                         | The lookup URL for Element Manager.                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Maximum Backup Files</b>                      | The maximum number of backup files that you can create. The valid values are 1 through 5, and the default is 3.<br><br>When the maximum limit is reached, the system rotates backup archives.                                                                                                                                                                                                                                   |
| <b>Maximum Data Retention Limit (days)</b>       | The maximum data retention limit in days. You can set the limit for any data retention rule.                                                                                                                                                                                                                                                                                                                                    |
| <b>Maximum size for log data stored</b>          | The maximum size for log data stored. This is the upper limit on the number of records on the log_store table.                                                                                                                                                                                                                                                                                                                  |
| <b>Maximum Transaction Timeout Limit (Hours)</b> | The maximum transaction timeout limit in hours.                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Remote Utility Directory</b>                  | The directory on the database server that contains the Element Manager backup or restore utilities.                                                                                                                                                                                                                                                                                                                             |
| <b>Scheduler URL</b>                             | The URL for gaining access to the Scheduler.                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Remote Server Password</b>                    | The password for accessing the SCP server.<br><br> <b>Important:</b><br>To use the <b>Use Default</b> option on the Backup or Restore page, ensure that you specify the following: <ul style="list-style-type: none"> <li>• Remote server IP</li> <li>• User name</li> <li>• Password</li> <li>• Name and path of the backup file</li> </ul> |

*Table continues...*



| Name                                  | Description                                                                                           |
|---------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Confirm Remote Server Password</b> | The SCP server password that you retype to confirm.<br>This field is only available in the Edit mode. |
| <b>Remote Server Port</b>             | The SSH port for the SCP server.                                                                      |
| <b>Remote server</b>                  | The hostname of the SCP server.                                                                       |
| <b>Remote Server User</b>             | The username to access the secure access server.                                                      |

| Button        | Description                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>   | Displays the Edit Profile: SMGR Element Manager page to edit the System Manager Element Manager profile parameters.                                               |
| <b>Done</b>   | Closes the View Profile: SMGR Element Manager page.                                                                                                               |
| <b>Commit</b> | Saves and commits any changes made in the System Manager Element Manager profile settings.<br>This field is only available in the Edit mode.                      |
| <b>Cancel</b> | Cancels any changes and reverts the System Manager Element Manager profile settings to the last saved settings.<br>This field is only available in the Edit mode. |

---

## View Profile:SNMP field descriptions

### Avaya IM System Manager subagent attributes

| Name                          | Description                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Master Agent IPAddress</b> | IP address of the machine on which master agent is running.                                                                                                                                                                                                                                                                             |
| <b>Master Agent TCP Port</b>  | The connection between master agent and subagent is established via a TCP port using AgentX protocol. This port has to be configured with both the master agent and the subagent so that the master agent starts listening on the configured TCP port and then the subagent establishes connection with the master agent via this port. |
| <b>Sub Agent IPAddress</b>    | IP address of the machine on which subagent is deployed.                                                                                                                                                                                                                                                                                |

---

## View Profile:Scheduler field descriptions

### Scheduler Feature

| Name                   | Description                                                               |
|------------------------|---------------------------------------------------------------------------|
| <b>Number Of Retry</b> | A count that defines the number of attempts to start the scheduler MBEAN. |
| <b>Retry Delay</b>     | Delay in time in seconds between each retry.                              |

## Scheduler Look Up Details

| Name                    | Description                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initial Context Factory | User name for secured Java Naming and Directory Interface (JNDI).                                                                                                                                                                                |
| Naming Server User Name |                                                                                                                                                                                                                                                  |
| Provider URL            | <p>The PROVIDER_URL which gives the server name and port on which a service is running.</p> <p> <b>Note:</b></p> <p>This parameter is currently not in use.</p> |

| Button | Description                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------|
| Edit   | Displays the Edit Profile:Scheduler page. Use this page to edit the parameters in the Scheduler profile. |
| Done   | Closes the View Profile:Scheduler page.                                                                  |

## Edit Profile:Scheduler field descriptions

### Scheduler Feature

| Name            | Description                                                               |
|-----------------|---------------------------------------------------------------------------|
| Number Of Retry | A count that defines the number of attempts to start the scheduler MBEAN. |
| Retry Delay     | Delay in time in seconds between each retry.                              |

## Scheduler Look Up Details

| Name                    | Description                                                                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Initial Context Factory | User name for secured Java Naming and Directory Interface (JNDI).                                                                                                                                                                                  |
| Naming Server User Name |                                                                                                                                                                                                                                                    |
| Provider URL            | <p>The PROVIDER_URL which gives the server name and port on which a service is running.</p> <p> <b>Note:</b></p> <p>This parameter is currently not in use.</p> |

| Button | Description                                                                        |
|--------|------------------------------------------------------------------------------------|
| Commit | Saves the changes to the database.                                                 |
| Cancel | Cancels the edit profile operation and returns to the View Profile:Scheduler page. |

## Configuring the TrapListener service

### Procedure

1. On the System Manager console, click **Services > Configurations**.
2. In the left navigation pane, click **Settings > SMGR**.
3. Click **TrapListener**.
4. On the View Profile: TrapListener Service page, click **Edit**.
5. Edit the required fields in the Edit Profile: TrapListener Service page.
6. Click **Commit**.

### Related links

[TrapListener service](#) on page 1030

[View Profile: TrapListener field descriptions](#) on page 889

## View Profile: TrapListener field descriptions

| Name                           | Description                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Password</b> | The password used to authenticate the user. The default is avaya123.                                                                                                                                                                                                                             |
| <b>Authentication Protocol</b> | The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The options are: <ul style="list-style-type: none"> <li>• <b>md5</b></li> <li>• <b>SHA</b></li> </ul> The default is <b>md5</b> .                                                                     |
| <b>Community</b>               | The community for TrapListener.                                                                                                                                                                                                                                                                  |
| <b>Email Forward</b>           | The option to forward the emails to the user. The default is <b>false</b> .<br>If set to <b>true</b> , the system forwards the emails to the user.                                                                                                                                               |
| <b>Email to addresses</b>      | A list of e-mail addresses, which are comma separated, to which alarms are forwarded.                                                                                                                                                                                                            |
| <b>Privacy Password</b>        | The password that you use to encrypt the SNMP data. The default is avaya123.                                                                                                                                                                                                                     |
| <b>Privacy Protocol</b>        | The encryption policy for an SNMP V3 user. The options are: <ul style="list-style-type: none"> <li>• <b>DES</b>: Use the DES encryption for the SNMP-based communication.</li> <li>• <b>AES</b>: Use the AES encryption for the SNMP-based communication.</li> </ul> The default is <b>AES</b> . |
| <b>TrapListener Port</b>       | The port on which TrapListener listens. The default is 10162. The field is read-only.                                                                                                                                                                                                            |

*Table continues...*

| Name               | Description                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>V3 UserName</b> | The SNMP V3 user name. The default is <b>initial</b> .<br><br>Although you can change the SNMP V3 user name, use the default value. |

 **Note:**

The system configures the **Privacy Password**, **Authentication Password**, **Users**, and **Community** fields with default values. You must change the values immediately after you deploy System Manager.

| Button        | Description                                                                                  |
|---------------|----------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes you have made in the <b>TrapListener Configuration Parameters</b> section. |
| <b>Cancel</b> | Cancels the edit and returns to the previous page.                                           |

## Configuring Trust Management

### Procedure

1. On the System Manager web console, click **Services > Configurations > Settings > SMGR > Trust Management**.
2. On the View Profile: Trust Management page, click **Edit**.
3. On the Edit Profile: Trust Management page, edit the required parameters.
4. Click **Commit**.

## View Profile: TrustManagement field descriptions

| Name                                                                              | Description                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Number of days after which system deletes expired certificates</b>             | The number of days after which System Manager deletes the expired certificates from the system. The default value is 365 days.<br><br>If the certificate expires before the number of configured days, System Manager purges the certificate. |
| <b>Threshold (in days) for raising an alarm for certificate expiration (1-60)</b> | The number of days before the certificate expiry when an alarm is generated.                                                                                                                                                                  |
| <b>Auto-renew Certificates (true/false)</b>                                       | The status of the auto-renewal of certificates from the Trust Management agent. Set this field to True if you want auto renewal of certificates.                                                                                              |
| <b>Threshold (in days) for triggering auto-renewal of certificates (1-60)</b>     | The number of days before the certificate expiry when the auto-renewal of certificates is triggered.                                                                                                                                          |

| Button      | Description                                        |
|-------------|----------------------------------------------------|
| <b>Edit</b> | Returns to the Edit Profile: TrustManagement page. |
| <b>Done</b> | Returns to the previous page.                      |

## Edit Profile: TrustManagement field descriptions

| Name                                                                              | Description                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Number of days after which system deletes expired certificates</b>             | The number of days after which System Manager deletes the expired certificates from the system. The default value is 365 days.<br>If the certificate expires before the number of configured days, System Manager purges the certificate. |
| <b>Threshold (in days) for raising an alarm for certificate expiration (1-60)</b> | The number of days before the certificate expiry when an alarm is generated.                                                                                                                                                              |
| <b>Auto-renew Certificates (true/false)</b>                                       | The status of the auto-renewal of certificates from the Trust Management agent. Set this field to True if you want auto renewal of certificates.                                                                                          |
| <b>Threshold (in days) for triggering auto-renewal of certificates (1-60)</b>     | The number of days before the certificate expiry when the auto-renewal of certificates is triggered.                                                                                                                                      |

| Button        | Description                                                   |
|---------------|---------------------------------------------------------------|
| <b>Commit</b> | Saves your changes in the Edit Profile: TrustManagement page. |
| <b>Cancel</b> | Cancels your changes and returns to the previous page.        |

## View Profile: User Bulk Import Profile field descriptions

### User Bulk Import Module

| Name                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Error Configuration</b>                     | <p>The value in this field specifies what action the system performs when an error is encountered during bulk importing users record in the system. The options are:</p> <ul style="list-style-type: none"> <li>• <b>True:</b> The system skips the erroneous record in the input file and continue to import other records. The default is <b>True</b>.</li> </ul> <p>If this parameter is set to true, the <b>Continue processing other records</b> option is set as the default in the <b>Select error configuration</b> field on the Import Users page.</p> <ul style="list-style-type: none"> <li>• <b>False:</b> The system aborts the import operation on encountering the first error in the input file.</li> </ul> <p>If this parameter is set to false, the <b>Abort on first error</b> option is set as default in the <b>Select error configuration</b> field on the Import Users page.</p> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b></p> |
| <b>Enable Error File Generation</b>                    | <p>The option to generate error file during the importing users job. The options are:</p> <ul style="list-style-type: none"> <li>• <b>True:</b> The system generates an error file for a failed import.</li> <li>• <b>False:</b> The system does not generate an error file for a failed import.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Maximum Number of Error records to be displayed</b> | <p>The maximum number of error records that the Job Details page can display for a user import job that has failed to import user records completely or partially.</p> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users &gt; View Job</b>.</p> <p>Select a failed job from the table before you click <b>View Job</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Maximum Number of Job records to be displayed</b>   | <p>The maximum number of job records that the system displays on the Import Users page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

*Table continues...*

| Name                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Action for a matching record</b> | <p>A default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: The system does not import user records from the input file that already exists in the database.<br/>If you enter 0, the <b>Skip</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• <b>1</b>: The system appends the records for an attribute.<br/>If you enter 1, the <b>Merge</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• <b>2</b>: The system replaces the record with the record in the input file if a matching record is found.<br/>If you enter 2, the <b>Replace</b> option is set as the default option for the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• <b>3</b>: The system deletes the records from the database that matches the records in the input file.<br/>If you enter 3, the <b>Delete</b> option is set as the default option for the <b>If a matching record already exists</b> field.</li> </ul> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b>.</p> |
| Button                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Edit</b>                                 | Displays the Edit Profile: User Bulk Import Profile page where you can change bulk import parameters of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Edit Profile: User Bulk Import Profile field descriptions

Use this page to modify the value of parameters that define settings for bulk importing users records.

## User Bulk Import Module

| Name                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Error Configuration</b>                     | <p>The action that the system performs when an error is encountered during bulk importing users record in the system. The options are:</p> <ul style="list-style-type: none"> <li>• <b>True:</b> The system skips the erroneous record in the input file and continue to import other records. This is the default value.</li> </ul> <p>If this parameter is set to true, the <b>Continue processing other records</b> option is set as the default option for the <b>Select error configuration</b> field on the Import Users page.</p> <ul style="list-style-type: none"> <li>• <b>False:</b> The system aborts the importing process on encountering the first error in the input file.</li> </ul> <p>If this parameter is set to false, the <b>Abort on first error</b> option is set as default option for the <b>Select error configuration</b> field on the Import Users page.</p> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b>.</p> |
| <b>Enable Error File Generation</b>                    | <p>The option to generate the error file for an import users job. The options are:</p> <ul style="list-style-type: none"> <li>• <b>True:</b> The system generates an error file for a failed import job.</li> <li>• <b>False:</b> The system does not generate an error file for a failed import job.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Maximum Number of Error records to be displayed</b> | <p>The maximum number of error records that the Job Details page can display for a user import job that has failed to import user records completely or partially.</p> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users &gt; View Job</b>.</p> <p>Select a failed job from the table before you click <b>View Job</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Maximum Number of Job records to be displayed</b>   | <p>The maximum number of job records that the system displays on the Import Users page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

*Table continues...*



| Name                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Action for a matching record</b> | <p>The default action that the system performs when the system finds a matching record in the database while bulk importing users. The options are:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: The system does not import user records from the input file that already exists in the database.<br/>If you enter 0, the <b>Skip</b> option is set as default in the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• <b>1</b>: The system appends the records for an attribute.<br/>If you enter 1, the <b>Merge</b> option is set as default in the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• <b>2</b>: The system replaces the record with the record in the input file if a matching record is found.<br/>If you enter 2, the <b>Replace</b> option is set as default in the <b>If a matching record already exists</b> field on the Import Users page.</li> <li>• <b>3</b>: The system deletes the records from the database that matches the records in the input file.<br/>If you enter 3, the <b>Delete</b> option is set as default in the <b>If a matching record already exists</b> field.</li> </ul> <p>To access the Import Users page, click <b>Manage Users &gt; More Actions &gt; Import Users</b>.</p> |
| Button                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Edit</b>                                 | Displays the Edit Profile:User Bulk Import Profile page where you can change the user bulk import parameters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

# Chapter 13: Managing inventory

---

## Element management

Inventory maintains a repository that records elements deployed on System Manager, including the runtime relationships. An element in the inventory refers to a single instance or clustered instance of a managed element. Inventory provides a mechanism for creating, modifying, searching, and deleting elements and the access point information from the repository. Inventory retrieves information about elements that are added or deleted from the repository.

Inventory integrates the adopting applications with the common console of System Manager. Through Inventory, elements can provide a link that redirects to the webpage of the element manager. Such links appear for only specific element types.

When you deploy an Avaya Aura® application by using Solution Deployment Manager, the system displays the application in the System Manager inventory.

To upgrade an Avaya Aura® application by using Solution Deployment Manager, you must add applications such as Communication Manager, Session Manager, and Branch Session Manager in the inventory.

 **Note:**

You must add Appliance Virtualization Platform or ESXi host from Application Management on Solution Deployment Manager. The system displays Appliance Virtualization Platform or ESXi host on the Manage Elements page.

 **Note:**

On the Manage Elements page, links to Corporate Directory, IPsec, Numbering Groups, Patches, Secure FTP Token, SNMP Profiles, and Software Deployment might not be active. You can gain access to the elements from **Users > Administrators**.

Using Manage Elements, you can add elements in the following methods:

- Manually add elements to the System Manager inventory.
- Perform automatic inventory collection from the Discovery tab that automatically adds elements to the System Manager inventory.
- Add elements to the System Manager inventory in bulk from the **More Actions > Import** link.

Using Manage Elements you can:

- Add or modify elements

- Delete elements
- Assign and remove entries for elements
- Provide a certificate to an element
- Replace a certificate
- Import elements in bulk
- Configure SAI Gateway
- Configure Avaya Services Registration
- View certificate add status

From Release 8.1, System Manager displays a progress bar on the Manage Elements for ongoing Geographic Redundancy event notification status that are sent to the elements that are added on System Manager. When you hover on the status bar, the system displays the event name for which this notification is being sent out from System Manager to elements. You can use the **More Actions > View Notification Status** page to view the details of this notification.

For System Manager Geographic Redundancy:

- Manage or unmanage elements
- Get current status of elements

### Manage Elements access

You require access to the **Inventory > Manage Elements** page on the System Manager web console. The role must have the following permissions assigned:

For resource type elements, all permissions in the **Role Resource Type Actions** section.

### Bulk import

Inventory supports the creation and updation of elements by importing data from an XML file. You can import elements only through the graphical user interface.

Inventory provides the following configuration options for each import operation:

- Abort on first error: The system stops the import operation if any exception occurs.
- Continue processing other records: The system does not stop the import operation even if any exception occurs, and the import operation continues.
- Replace: Reimports all data for the element that you import. The replace function replaces an element and the related data with a new one.
- Merge: Merges the data of an element with the import data from an input XML file.
- Skip: Skips the import operation. As an administrator, you reimport the elements to recover from failures. If you reimport the same file to recover from failures, RTS does not overwrite any record that you have successfully added. Inventory continues to process other records from the file.
- Delete: Deletes an element.
- Schedule: Schedules the import of the element.

---

## Methods to add elements to System Manager

---

### Manual addition of elements

You can manually add an element to the System Manager inventory from the Manage Elements page. For example, Communication Manager.

You must add the ESXi host from Application Management on Solution Deployment Manager. The system displays the ESXi host on the Manage Elements page.

---

### Adding a new element

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click the element type that you want to create.
5. On the New <element-name> page, on the **General** and **Attributes** tabs, complete the required fields.

The tabs and fields on the New <element-name> page varies based on the application that you select

6. Click **Commit**.

System Manager creates the element and displays on the Manage Elements page.

#### Related links

[Element details field descriptions](#) on page 936

---

### Bulk import of elements

You can add elements to the System Manager inventory in bulk from the Manage Elements page, by using the **More Actions > Import** link.

### Importing elements

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.

3. On the Manage Elements page, click **More Actions > Import**.
4. On the Import Elements page, click **Browse** to select the XML file that you want to import.
5. Click **Import**.

---

## Discovering elements

### Discovery of Avaya Aura® applications and associated devices

To manage and upgrade software from System Manager, you must discover elements in the network. The system performs the discovery by using discovery profiles, where you configure subnetwork, SNMP access profiles, and element types to be discovered.

On the Discovery tab of **Inventory > Manage Elements**, you can create discovery profiles and use the profiles to discover elements. The Manage Elements page displays the discovered elements.

You must configure the applicable discovery parameters for System Manager to discover the Avaya Aura® application. System Manager uses SNMPv1 or SNMPv3 to discover Avaya Aura® applications.

For applications such as Communication Manager, you can use SNMP discovery or add the application from Manage Elements.

 **Note:**

To upgrade an Avaya Aura® application by using Solution Deployment Manager, discovery of applications, such as Communication Manager, Session Manager, and Branch Session Manager is a mandatory task.

### Creating discovery profiles and discovering elements

#### Before you begin

Configure the subnetwork profiles, SNMP profiles, and element type profiles on the **Discovery** tab by using the links available at the beginning of the Discovery Profile List page or from the following links:

- **Inventory > Subnet Configuration**
- **Inventory > Element Type Configuration**
- **Configurations > Settings > SMGR > Global SNMP Configuration**

#### About this task

You can create discovery profiles and use the profiles to discover elements in System Manager. The Manage Elements page displays the discovered elements.

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.

3. Click the **Discovery** tab.

The system displays the Discovery Profile List page.

4. Click **New**.

The system displays the Create Discovery Profile page.

5. In the **Discovery Profile Name** field, type a name for the discovery profile.

6. In the **Subnet Configurations** section, perform the following:

- a. Click a subnetwork that you configured in **Inventory > Subnet Configuration**.
- b. Click an element type that you configured on **Inventory > Element Type Configuration**.

The **Discovery Element Type Access Profiles** column displays all access profiles of an element type.

- c. To select or clear profiles, in the **Choose Element Type Access Profiles** column, click **Choose Element Access**.
- d. In the **Profile List** section, click the global SNMP profile that you configured on **Configurations > Settings > SMGR > Global SNMP Configuration**.

7. Click **Commit**.

The system displays the new discovery profile on the Discovery Profile List page in the **Discovery Profiles** section.

8. Select the discovery profile and perform one of the following:

- Click **Discover Now**.
- To discover the element later, click **Schedule Discovery**, and provide the date and time when the discovery must run.

The system displays a dialog box with the message `Discovery is Running` and the number of elements that are discovered. The system lists the discovered elements on the Manage Elements page in the **Elements** section. The system closes the dialog box when the discovery is complete.

While the discovery is in progress, the system blocks any action that you perform on the **Discovery** tab.

## Related links

[Device list](#) on page 901

[Discovery Profile List field descriptions](#) on page 901

[Element Access Profile Management field descriptions](#) on page 911

[Subnet Configurations field descriptions](#) on page 909

[SNMP Access Profiles field descriptions](#) on page 905

[Create or Edit Discovery Profile field descriptions](#) on page 902

## Device list

The table lists the minimum requirements for an SNMP discovery. For successful discovery, you must configure the following on the Avaya equipment.

| Device for discovery                    | Protocol used     | Ports used        | Access                        | Notes                                                        |
|-----------------------------------------|-------------------|-------------------|-------------------------------|--------------------------------------------------------------|
| Communication Manager                   | SNMPv1 and SNMPv3 | SSH to 22 or 5022 | Direct                        | -                                                            |
| Session Manager, Branch Session Manager | SNMPv1 and SNMPv3 | SSH to 22 or 5022 | Direct                        |                                                              |
| Appliance Virtualization Platform       | SNMPv1 and SNMPv3 |                   | Direct                        | Manually added from Application Management                   |
| Avaya Breeze <sup>®</sup> platform      |                   |                   |                               |                                                              |
| Application Enablement Services         |                   |                   |                               |                                                              |
| IP Office                               | SNMPv1            | -                 | -                             | -                                                            |
| CLAN (TN799DP)                          | SNMPv1            | -                 | Direct                        | Static community publicclan read-only and read-write strings |
| MedPro (TN2302, TN2602)                 | SNMPv1            | -                 | Through Communication Manager | -                                                            |
| G250, G350                              | SNMPv1 and SNMPv3 | SSH to 22         | Direct                        | -                                                            |
| G430, G450                              | SNMPv1 and SNMPv3 | SSH to 22         | Direct                        | -                                                            |
| G700                                    | SNMPv1            | -                 | Direct                        | -                                                            |

## Discovery Profile List field descriptions

### Discovery Profiles

| Name                     | Description                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Discovery Profile</b> | The name of the discovery profile.                                                                                                                           |
| <b>Subnet Profiles</b>   | The name of the subnetwork profile.<br><br>For each subnetwork profile name, the system provides a cut-through that displays the subnetwork profile details. |

*Table continues...*

| Name                   | Description                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access Profiles</b> | The name of the access profile.<br><br>For each access profile name, the system provides a cut-through that displays the access profile details. |
| <b>Element Types</b>   | The element type.                                                                                                                                |

### Discovery Job Status

| Name              | Description                                   |
|-------------------|-----------------------------------------------|
| <b>Job Name</b>   | The name of the discovery job.                |
| <b>Start Time</b> | The start date and time of the discovery job. |
| <b>End Time</b>   | The end date and time of the discovery job.   |
| <b>Status</b>     | The current status of the discovery job.      |

| Button                    | Description                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------|
| <b>New</b>                | Displays the Create Discovery Profile page where you create a new discovery profile.                |
| <b>Edit</b>               | Displays the Edit Discovery Profile page where you can change the discovery profile information.    |
| <b>Delete</b>             | Displays the Discovery Profile Delete Confirmation page where you can delete the discovery profile. |
| <b>Discover Now</b>       | Starts the process of discovering the element.                                                      |
| <b>Schedule Discovery</b> | Schedules the discovery process to run at the specified time.                                       |

### Create or Edit Discovery Profile field descriptions

| Name                          | Description                        |
|-------------------------------|------------------------------------|
| <b>Discovery Profile Name</b> | The name of the discovery profile. |

### Subnet Configurations

| Name                                | Description                                        |
|-------------------------------------|----------------------------------------------------|
| <b>Name</b>                         | The name of the subnetwork.                        |
| <b>IPAddress</b>                    | The IP address of the subnetwork.                  |
| <b>Mask/Network Prefix</b>          | The IP subnetwork mask prefix.                     |
| <b>No. of IPs to scan in subnet</b> | The number of IPs to be scanned in the subnetwork. |

### Element Type Access Profiles

| Name                 | Description       |
|----------------------|-------------------|
| <b>Element Types</b> | The element type. |

*Table continues...*



| Name                                          | Description                                                                                                                                   |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Discovery Element Type Access Profiles</b> | The discovery profiles for the element type access.                                                                                           |
| <b>Choose Element Type Access Profiles</b>    | The link to the <b>Element Type Access Profiles</b> section where you can select or clear the discovery profiles for the element type access. |

## Profile List

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>    | The name of the profile.                                                                                                                                                                                                                                                                                                                                     |
| <b>Type</b>            | The SNMP protocol type. The options are V1 and V3.                                                                                                                                                                                                                                                                                                           |
| <b>Read Community</b>  | The read community of the device.<br><b>Read Community</b> applies only to the SNMP V1 protocol.                                                                                                                                                                                                                                                             |
| <b>Write Community</b> | The write community of the device.<br><b>Write Community</b> applies only to the SNMP V1 protocol.                                                                                                                                                                                                                                                           |
| <b>User</b>            | The user name of the SNMP V3 protocol operation.                                                                                                                                                                                                                                                                                                             |
| <b>Auth Type</b>       | The authentication protocol to authenticate the source of traffic from SNMP V3 users. The options are: <ul style="list-style-type: none"> <li>• <b>MD5</b><br/>The default is <b>MD5</b>.</li> <li>• <b>SHA</b></li> <li>• <b>None</b></li> </ul> <b>Auth Type</b> applies only to the SNMP V3 protocol.                                                     |
| <b>Priv Type</b>       | The encryption policy for an SNMP V3 user. The options are: <ul style="list-style-type: none"> <li>• <b>DES</b>: For SNMP-based communication.<br/>The default is <b>DES</b>.</li> <li>• <b>AES</b>: For SNMP-based communication.</li> <li>• <b>None</b>: Does not encrypt traffic for this user.</li> </ul> Set <b>Priv Type</b> only for an SNMP V3 user. |
| <b>Privileges</b>      | The privileges that determine the operations that you can perform on MIBs. <ul style="list-style-type: none"> <li>• <b>Read/Write</b>: To perform the GET and SET operations.</li> <li>• <b>Read</b>: To perform only the GET operation.</li> <li>• <b>None</b></li> </ul> The default is <b>None</b> .                                                      |
| <b>Timeout</b>         | The time in milliseconds for which the element waits for a response from the device that the element polls.                                                                                                                                                                                                                                                  |

*Table continues...*

| Name               | Description                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Retries</b>     | The number of times that the element polls a device and fails to receive a response. After the retries, the element times out. |
| <b>Description</b> | A brief description of the profile.                                                                                            |

| Button        | Description                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes that you make on the Create Discovery Profile or Edit Discovery Profile page. |

## Managing SNMP Access Profiles

### Adding an SNMP access profile

#### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR > Global SNMP Configuration**.
3. Click **New**.
4. On the New SNMP Access Profile page, perform the following:
  - a. In the **Type** field, click the type of the SNMP protocol.  
For more information, see SNMP Access Profile field descriptions.
  - b. In the **Profile Name** and **Description** fields, type the name of the profile and a description.
  - c. Complete the remaining fields on the page.
5. Click **Commit**.

#### Related links

[SNMP Access Profile field descriptions](#) on page 906

[SNMP Access Profiles field descriptions](#) on page 905

### Editing the SNMP access profile

#### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR > Global SNMP Configuration**.
3. In the profile list, select the SNMP access profile that you want to change.
4. Click **Edit**.
5. On the Edit SNMP Access Profile page, change the details as appropriate.  
For more information, see SNMP Access Profile field descriptions.
6. Click **Commit**.

#### Related links

[SNMP Access Profile field descriptions](#) on page 906

[SNMP Access Profiles field descriptions](#) on page 905

## Deleting an SNMP access profile

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR > Global SNMP Configuration**.
3. In the profile list, click the SNMP access profile that you want to delete.
4. Click **Delete**.
5. On the Snmp Access Profile/s Delete Confirmation page, click **Delete** to confirm the deletion.

## SNMP Access Profiles field descriptions

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>    | The name of the profile.                                                                                                                                                                                                                                                                                                                                          |
| <b>Type</b>            | The SNMP protocol type. The options are V1 and V3.                                                                                                                                                                                                                                                                                                                |
| <b>Read Community</b>  | The read community of the device.<br><b>Read Community</b> applies only to the SNMP V1 protocol.                                                                                                                                                                                                                                                                  |
| <b>Write Community</b> | The write community of the device.<br><b>Write Community</b> applies only to the SNMP V1 protocol.                                                                                                                                                                                                                                                                |
| <b>User</b>            | The user name of the SNMP V3 protocol operation.                                                                                                                                                                                                                                                                                                                  |
| <b>Auth Type</b>       | The authentication protocol to authenticate the source of traffic from SNMP V3 users. The options are: <ul style="list-style-type: none"> <li>• <b>MD5</b></li> <li>The default is <b>MD5</b>.</li> <li>• <b>SHA</b></li> <li>• <b>None</b></li> </ul> <b>Auth Type</b> applies only to the SNMP V3 protocol.                                                     |
| <b>Priv Type</b>       | The encryption policy for an SNMP V3 user. The options are: <ul style="list-style-type: none"> <li>• <b>DES</b>: For SNMP-based communication.</li> <li>The default is <b>DES</b>.</li> <li>• <b>AES</b>: For SNMP-based communication.</li> <li>• <b>None</b>: Does not encrypt traffic for this user.</li> </ul> Set <b>Priv Type</b> only for an SNMP V3 user. |

*Table continues...*

| Name               | Description                                                                                                                                                                                                                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Privileges</b>  | <p>The privileges that determine the operations that you can perform on MIBs.</p> <ul style="list-style-type: none"> <li>• <b>Read/Write</b>: To perform the GET and SET operations.</li> <li>• <b>Read</b>: To perform only the GET operation.</li> <li>• <b>None</b></li> </ul> <p>The default is <b>None</b>.</p> |
| <b>Timeout</b>     | The time in milliseconds for which the element waits for a response from the device that the element polls.                                                                                                                                                                                                          |
| <b>Retries</b>     | The number of times that the element polls a device and fails to receive a response. After the retries, the element times out.                                                                                                                                                                                       |
| <b>Description</b> | A brief description of the profile.                                                                                                                                                                                                                                                                                  |

| Button        | Description                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>New</b>    | Displays the New SNMP Access Profile page where you can add a new SNMP access profile.                                |
| <b>Edit</b>   | Displays the Edit SNMP Access Profile page where you can change an SNMP access profile.                               |
| <b>Delete</b> | Displays the Snmp Access Profile/s Delete Confirmation page where you can confirm the deletion of the access profile. |

## SNMP Access Profile field descriptions

### For SNMP protocol V3

The system displays the following fields when you click **V3** in the **Type** field:

| Name                       | Description                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>        | The name of the profile.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>         | A brief description of the profile.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Type</b>                | The SNMP protocol type.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>User</b>                | The user name as defined in the element.                                                                                                                                                                                                                                                                                                                                                 |
| <b>Authentication Type</b> | <p>The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>MD5</b></li> </ul> <p>The default is <b>MD5</b>.</p> <ul style="list-style-type: none"> <li>• <b>SHA</b></li> <li>• <b>None</b></li> </ul> <p><b>Authorization Type</b> applies only to the SNMP V3 protocol.</p> |

*Table continues...*

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Password</b>         | The password to authenticate the user. The password must contain at least eight characters.<br><br>* <b>Note:</b><br>The password is mandatory.                                                                                                                                                                                                                                                                                                                             |
| <b>Confirm Authentication Password</b> | The SNMP V3 protocol authentication password that you retype for confirmation.                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Privacy Type</b>                    | The encryption policy for an SNMP V3 user. The possible values are:<br><ul style="list-style-type: none"> <li>• <b>AES</b>: For SNMP-based communication.</li> <li>• <b>AES128</b>: For SNMP-based communication.</li> <li>• <b>DES</b>: For SNMP-based communication.</li> </ul> The default is <b>DES</b> .<br><ul style="list-style-type: none"> <li>• <b>None</b>: Does not encrypt traffic for this user.</li> </ul> Set <b>Privacy Type</b> only for an SNMP V3 user. |
| <b>Privacy Password</b>                | The password used to enable the <b>DES</b> or <b>AES</b> encryption. DES passwords must contain at least eight characters.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Confirm Privacy Password</b>        | The privacy password that you retype for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Privileges</b>                      | The privileges that determine the operations that you can perform on MIBs.<br><ul style="list-style-type: none"> <li>• <b>None</b><br/>The default is None.</li> <li>• <b>Read/Write</b>: To perform GET and SET operations.</li> <li>• <b>Read</b>: To perform only the GET operation.</li> </ul>                                                                                                                                                                          |
| <b>Timeout</b>                         | The time in milliseconds for which the element waits for a response from the device being polled during discovery.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Retries</b>                         | The number of times that the element polls a device without receiving a response before timing out.                                                                                                                                                                                                                                                                                                                                                                         |

### For SNMP protocol V1

The system displays the following fields when you click **V1** in the **Type** field:

| Name                | Description                         |
|---------------------|-------------------------------------|
| <b>Profile Name</b> | The name of the profile.            |
| <b>Description</b>  | A brief description of the profile. |

*Table continues...*

| Name                   | Description                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Type</b>            | The SNMP protocol type.<br><br>* <b>Note:</b><br>To upgrade Communication Manager using SNMP protocol, you must select SNMPV1. |
| <b>Read Community</b>  | The read community of the device.<br><b>Read Community</b> applies only to the SNMP V1 protocol.                               |
| <b>Write Community</b> | The write community of the device.<br><b>Write Community</b> applies only to the SNMP V1 protocol.                             |
| <b>Timeout</b>         | The time in milliseconds for which the element waits for a response from the device that the element polls.                    |
| <b>Retries</b>         | The number of times that the element polls a device and fails to receive a response. After the retries, the element times out. |

| Button        | Description                                                               |
|---------------|---------------------------------------------------------------------------|
| <b>Commit</b> | Adds or edits the SNMP access profile depending on the option you select. |
| <b>Cancel</b> | Returns to the previous page.                                             |

## Configuring subnets

### Adding a subnetwork Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Subnet Configuration**.
3. On the Subnet Configurations page, click **New**.  
The system adds a new row where you can add the details.
4. Type the name, IP address, and subnetwork mask.
5. Click **Save**.
6. To add more than one subnetworks, repeat Step 3.

### Related links

[Subnet Configurations field descriptions](#) on page 909

### Editing the subnetwork Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Subnet Configuration**.
3. On the Subnet Configurations page, select the subnetwork that you want to change.

4. Change the name, IP address, and subnetwork mask as appropriate.
5. Repeat Step 3 to change the information for more than one subnetworks.
6. Click **Save**.

### Related links

[Subnet Configurations field descriptions](#) on page 909

## Deleting a subnetwork

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Subnet Configuration**.
3. On the Subnet Configurations page, select the subnetworks that you want to delete.
4. Click **Delete**.
5. To confirm the deletion, click **Delete**.

The system deletes the subnetwork.

## Subnet Configurations field descriptions

| Name                                | Description                                        |
|-------------------------------------|----------------------------------------------------|
| <b>Name</b>                         | The name of the subnetwork.                        |
| <b>IPaddress</b>                    | The IP address of the subnetwork.                  |
| <b>Mask/Network Prefix</b>          | The IP subnetwork mask prefix.                     |
| <b>No. of IPs to scan in subnet</b> | The number of IPs to be scanned in the subnetwork. |

| Button        | Description                                                                              |
|---------------|------------------------------------------------------------------------------------------|
| <b>New</b>    | Adds a new row where you can provide the details of the subnetwork that you want to add. |
| <b>Delete</b> | Deletes a subnetwork.                                                                    |

| Button        | Description                   |
|---------------|-------------------------------|
| <b>Save</b>   | Adds or edits the subnetwork. |
| <b>Cancel</b> | Cancels your current action.  |

## Managing Element Access Profile

### Adding an element access profile

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Element Type Access**.
3. On the Element Access Profile Management page, in the **Element Type** field, click an element to which you want to provide access.

For more information, see Element Access Profile Management field descriptions.

4. Click **New**.
5. On the Access Profile Entry page, in the **Protocol** field, click a protocol.
6. Click **Commit**.

#### Related links

[Modify Access Profile Entry field descriptions](#) on page 911

[Element Access Profile Management field descriptions](#) on page 911

### Editing an element access profile

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Element Type Access**.
3. On the Element Access Profile Management page, in the **Element Access Profiles** section, select an element access profile that you want to edit.

For more information, see Element Access Profile Management field descriptions.

4. Perform one of the following:
  - Click **Edit**.
  - Click **View**, and on the View Access Profile Entry page, click **Edit**.
5. On the Modify Access Profile Entry page, change the appropriate fields.
6. Click **Commit**.

#### Related links

[Modify Access Profile Entry field descriptions](#) on page 911

[Element Access Profile Management field descriptions](#) on page 911

### Deleting an element access profile

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Element Type Access**.
3. On the Element Access Profile Management page, in the **Element Access Profiles** section, select an element access profile that you want to delete.

For more information, see Element Access Profile Management field descriptions.

4. Click **Delete**.
5. On the Confirmation page, click **Continue**.

The system deletes the element access profile from the **Element Access Profiles** section.



## Element Access Profile Management field descriptions

| Name                   | Description                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Element Type</b>    | The type of the element for which you want to provide the access.                                                         |
| <b>Name</b>            | The name of the element.                                                                                                  |
| <b>Protocol</b>        | The protocol that you use to access the element.                                                                          |
| <b>Login User Name</b> | The login name of the user as configured on the element.                                                                  |
| <b>System Profile</b>  | The system protocol. The available options are: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> |

| Button        | Description                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------|
| <b>New</b>    | Displays the Add Access Profile Entry page where you can add a new access profile for the element.  |
| <b>View</b>   | Displays the View Access Profile Entry page where you can view the access profile of an element.    |
| <b>Edit</b>   | Displays the Modify Access Profile Entry page where you can change an access profile of an element. |
| <b>Delete</b> | Deletes the access profile of an element that you select.                                           |

## Modify Access Profile Entry field descriptions

| Name               | Description                                                              |
|--------------------|--------------------------------------------------------------------------|
| <b>Protocol</b>    | The protocol that you use to access the element. The field is read-only. |
| <b>Name</b>        | The name of the element access profile.                                  |
| <b>Description</b> | A description of the element access profile.                             |
| <b>URI</b>         | The URI to reach the element access profile.                             |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>Commit</b> | Commits the changes that you made to element access details.                         |
| <b>Cancel</b> | Cancels the modify action and returns to the Element Access Profile Management page. |

## Create profiles and discover SRS and SCS servers

### Discover SRS and SCS servers

Use the **Create Profiles and Discover SRS/SCS** option to automatically discover survivable remote servers (SRS) and survivable core servers (SCS) from the main Communication Manager. System Manager uses the `list survivable-processor` command to discover the SRS and SCS servers that are associated with the main Communication Manager. The servers that are discovered are stored in **Manage Elements**.

Additionally, the SRS and SCS servers are automatically added in the System Manager inventory. The Communication Manager servers are automatically identified as survivable servers in **Inventory**.

## Creating profiles and discovering SRS and SCS servers

### Before you begin

Create the login profiles for Communication Manager devices with the **Element Type Configuration** option.

### About this task

Use the **Create Profiles and Discover SRS/SCS servers** option to create login profiles for devices, and use the login profiles to discover the Communication Manager devices.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Create Profiles and Discover SRS/SCS**.
3. On the Create Profiles and Discover SRS/SCS page, in **Select Devices to Create Profiles** table, select the devices for which you want to discover and create the login profile.
4. In **Select Profiles to Create on Devices**, select the login profile.
5. Select the **Discover SRS/SCS and Create Profile on SRS/SCS** option.
6. Perform one of the following actions:
  - Click **Now** to create the login profile and discover the device.
  - Click **Schedule** to schedule the login profile creation and device discovery at a later time.

### Related links

[Create Profiles and Discover SRS/SCS server field descriptions](#) on page 914

## Overwriting login profiles on devices

### Before you begin

You must create login profiles for Communication Manager devices with the **Element Type Configuration** option.

### About this task

Perform this task to overwrite profiles that exist on the devices.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Create Profiles and Discover SRS/SCS**.

3. On the Collected Inventory page, in the **Select Devices to Create Profiles** table, perform the following actions.
  - a. Select the devices for which you want to overwrite the login profile to discover the SRS and the SCS server.
  - b. Select **Add to Manage Elements** for the devices that you have selected.
4. In the **Select Profiles to Create on Devices** table, perform the following actions:
  - a. Select the new profile that you want to assign.
  - b. Select the **Add to Manage Elements** for the profiles that you have selected.
5. Select the **Overwrite Profiles on Devices** option.
6. Perform one of the following actions:
  - Click **Now** to overwrite the profile that you selected on the devices.
  - Click **Schedule** to overwrite the profile at a later time.

#### Related links

[Create Profiles and Discover SRS/SCS server field descriptions](#) on page 914

### Resetting the password

#### About this task

Perform this task to reset the password for a profile on the device.

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Create Profiles and Discover SRS/SCS**.
3. On the Collected Inventory page, in the **Select Devices to Create Profiles** table, perform the following actions.
  - a. Select the devices for which you want to overwrite the login profile to discover the SRS and the SCS server.
  - b. Select **Add to Manage Elements** for the devices that you have selected.
4. Select the **Reset Password** option.
5. Perform one of the following actions:
  - Select **Use Profile Password** to reset the password.
  - Select **Auto Generate Password** to automatically generate a password.
6. Perform one of the following actions:
  - Click **Now** to reset the password.
  - Click **Schedule** to reset the password at a later time.

#### Related links

[Create Profiles and Discover SRS/SCS server field descriptions](#) on page 914

## Create Profiles and Discover SRS/SCS server field descriptions

### Select Devices to Create Profiles

| Name                             | Description                                       |
|----------------------------------|---------------------------------------------------|
| <b>Name</b>                      | The name of the device.                           |
| <b>IP</b>                        | The IP address of the device.                     |
| <b>Family</b>                    | The device family to which the device belongs to. |
| <b>Type</b>                      | The device type.                                  |
| <b>Login Profile</b>             | The existing login profile for the device.        |
| <b>Software/Firmware Version</b> | The firmware version for the device.              |
| <b>Hardware Version</b>          | The hardware version of the device.               |
| <b>Module</b>                    | The device module.                                |
| <b>Description</b>               | The description you choose to add for the device. |
| <b>Location</b>                  | The location of the device.                       |
| <b>Serial Number</b>             | The serial number of the device.                  |

### Select Profiles to Create on Devices

| Name                                  | Description                                                      |
|---------------------------------------|------------------------------------------------------------------|
| <b>Profile Type</b>                   | The type of profile. Possible values include: SSH, SNMP, CM, GW. |
| <b>Profile Name/IP</b>                | The name of the profile.                                         |
| <b>CM Profile Type/SNMP V3 Groups</b> | The SNMP V3 profile type.                                        |
| <b>Add to Manage Elements</b>         | The option to add this profile in <b>Manage Elements</b> .       |

| Name                                                  | Description                                                   |
|-------------------------------------------------------|---------------------------------------------------------------|
| <b>Discover SRS/SCS and Create Profile on SRS/SCS</b> | Create the login profile and discovers the SRS or SCS server. |
| <b>Overwrite Profiles on Devices</b>                  | Overwrite the existing profile on the device.                 |
| <b>Reset Password</b>                                 | Reset the password of the existing profile.                   |

| Button          | Description                                                                          |
|-----------------|--------------------------------------------------------------------------------------|
| <b>Now</b>      | Performs the discovery, overwrite profile, or reset password action.                 |
| <b>Schedule</b> | Performs the discovery, overwrite profile, or reset password action at a later time. |

---

## Working with Elements in System Manager

---

### Additional information required for creating the Communication Manager or Messaging element

#### Communication Manager element

When you add the Communication Manager element from **Inventory > Manage Elements**, the element in turn starts a synchronization job in the background to bring all the relevant data from the elements to the System Manager database. To check the status of this synchronization job on System Manager Web Console, navigate to **System Manager Data > Scheduler** or reach the log files on the System Manager server.

#### Messaging element

If you are creating the Messaging element:

- The FQDN or IP address details in the **Node** field for a Messaging element must correspond to that of Messaging Storage Server (MSS) and not Messaging Application Server (MAS).
- Before adding the Messaging server in the System Manager applications, add the System Manager server details in the Trusted Server list on the Messaging server on the Messaging Administration/ Trusted Servers screen.
- The login credentials between the Messaging server trusted servers screen and the Session Manager application, entity, or attributes for a Messaging type of application must match.
- The **Trusted Server Name** field on the Trusted Server page maps to the **Login** field in the Attributes section. Similarly, the **Password** field on the Trusted Server page maps to the **Password** field in the Attributes section.
- To allow LDAP access to this Messaging server from the trusted server that you add, set the **LDAP Access Allowed** field on the Trusted Server page to **Yes**.

---

### Manage elements in System Manager configured with Geographic Redundancy

The primary or the secondary System Manager server can manage a GR-aware element. However, only the primary System Manager server manages the GR-unaware element. You must know the elements that each System Manager manages during the scenario such as normal operation and split network.

#### Related links

[Determining the System Manager that manages a GR-aware element](#) on page 916

---

## Determining the System Manager that manages a GR-aware element

### Before you begin

Log on to the System Manager web console of the primary server.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Verify the status of the elements in the **Managed by** column:
  - For GR-unaware elements, the system must display Not Supported.
  - For GR-aware elements, the system must display one of the following status:
    - Primary: Indicates that the primary System Manager manages the element.
    - Secondary: Indicates that the secondary System Manager manages the element.
    - Unknown: Indicates that the manageability status of the element is unavailable.
    - Unmanaged: Indicates that the current System Manager does not manage the element.
  - To refresh the **Managed by** status for an element, click **Get Current Status**.
  - To make the System Manager manage an element, the administrator must click **More Actions > Manage**.

For example, for managing Session Manager in a Geographic Redundancy setup, see *Administering Avaya Aura® Session Manager*.

---

## Viewing details of an element

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element.
4. Click **View**.

The system displays the details of the selected element.

---

## Modifying an element

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element.
4. Perform one of the following:
  - Click **Edit**.
  - Click **View > Edit**.

 **Note:**

If the Communication Manager system that you require to edit contains a : (colon) character in the name, the system disables the **Edit** button. Remove the : character from the Communication Manager name to enable **Edit**.

5. On the Edit <element name> page, modify the required fields.
6. Click **Commit**.

The system saves the changes.

---

## Deleting an element

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element.
4. Click **Delete**.
5. On the Delete Application Confirmation page, click **Delete**.

---

## Exporting elements from the System Manager command line interface

### About this task

Use the bulk export utility to export system records of an element to an xml file. The System Manager installer creates the `bulkExport` folder in the `<MGMT_HOME>\rts\` location.

### Before you begin

- Ensure that System Manager is installed and the server is running.

The bulk export utility requires System Manager to include runtime libraries.

- Ensure that JBoss is installed on the same server where you run the export utility.

## Procedure

1. Start an SSH session.
2. Log in to the System Manager server by using the command line interface.
3. To navigate to the `bulkExport` directory, type `cd <MGMT_HOME>\rts\bulkExport`.
4. Run the following command:

```
sh ./runRTSCli.sh [-u username] [-w password] [-p filePrefix] [-c perFileRecords]
[-ddestinationFolder] [-n application-type-name] [-v application-type-version]
```

The element generates a zip file with `filePrefix` as prefix and contains the xml data file in the destination folder. The system generates log files in the `/var/log/Avaya/mgmt/logs/rtsutility.log` location.

For example, `sh ./runRTSCli.sh -c 100 -d ./ -p rts -u admin -w System$987`.

5. (Optional) Change the log configuration in the `<MGMT_HOME>\rts\bulkExport\conf\log4.properties` file.

## Related links

[runRTSCli.sh command](#) on page 918

## runRTSCli.sh command

The `runRTSCli.sh` utility exports element system records to an xml file.

### Syntax

```
sh ./runRTSCli.sh [-u username] [-w password] [-p filePrefix] [-c perFileRecords] [-ddestinationFolder] [-n application-type-name] [-v application-type-version]
```

|                                                                     |                                                                          |
|---------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>-c,--numberOfRecordsPerFile</b><br><i>numberOfRecordsPerFile</i> | The number of records in a file.                                         |
| <b>-d,--output-directory</b> <i>destinationFolder</i>               | The name of the output folder.                                           |
| <b>-f,--config-file</b> <i>configurationFile</i>                    | The configuration file if you do not use the default configuration file. |
| <b>-h,--help</b>                                                    | The option to print help options.                                        |
| <b>-n,--application-type-name</b><br><i>applicationTypeName</i>     | The element type name. The parameter is optional.                        |
| <b>-p,--filename-prefix</b> <i>filePrefix</i>                       | The prefix for the zip file.                                             |
| <b>-s,--ssl</b>                                                     | Secure. The parameter is optional.                                       |



|                                                                    |                                                  |
|--------------------------------------------------------------------|--------------------------------------------------|
| <b>-u,--username</b> <i>System ManagerUsername</i>                 | System Manager username.                         |
| <b>-v,--application-type-version</b> <i>applicationTypeVersion</i> | Element type version. The parameter is optional. |
| <b>-w,--password</b> <i>System ManagerPassword</i>                 | System Manager password.                         |

### Return values

A zip file that contains an xml file with element system data.

### Description

The export utility generates a zip file with the specified prefix. The file contains the xml data file in the destination folder.

### Example

The example command creates the element data in the `rtsFileName` zip file with 100 records in the root folder `./`.

```
cd Mgmt_Home\rts\bulkExport
sh ./runRTSCli.sh -c 100 -d ./ -p rts -u admin -w System$987
```

### Files

The following files are associated with the `runRTSCli.sh` command:

- `<MGMT_HOME>\rts\bulkExport`: Location where you run the command.
- `/var/log/Avaya/mgmt/logs/rtsutility.log`: Location where the system generates the log files.
- `<MGMT_HOME>\rts\bulkExport\conf\log4.properties`: The properties file where you can change the log configuration.

---

## Assigning elements to an element

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
  - Select an element and click **Edit**.
  - To assign elements to an existing element in the view mode, select an element and click **View > Edit**.
4. In the Assign elements area, click **Assign elements**.
5. On the Assign elements page, select elements and click **Assign**.

 **Note:**

Assignment name for Communication Manager must match the switch connection on the Edit Application Enablement Services:<name> page. If the assignment name is blank, the system does not establish the SSL connection between Presence and AES.

---

## Removing assigned elements

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps to remove assigned elements from an existing element:
  - Select an element and click **Edit**.
  - Select an element and click **View > Edit**.
4. Select the elements that you must remove and click **Unassign Elements** in the Assign Elements section.

---

## Managing access profiles and ports

### Creating an access profile

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, do one of the following:
  - Click **New**.
  - To create an access profile for an existing element, click the element, and then click **Edit** or **View > Edit**.
4. On the **General** tab, in the **Access Profile** section, click **New**.

System Manager displays the Application System Supported Protocol and Access Profile Details sections.
5. In the Application System Supported Protocol section, in the **Protocol** field, select a protocol.

The options are:

  - **URI**: For system web services API.
  - **SSH**: For application upgrade functions.

- **SNMP**: For discovering elements.

Based on the protocol selection, System Manager displays the fields in the **Access Profile Details** section.

6. Enter the information about the access profile in the mandatory fields.
7. Click **Save**.

## Modifying an access profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **Edit** or **View > Edit**.
4. In the **Access Profile** section, select the access profile that you want to change and click **Edit**.
5. Modify the access profile information in the fields.
6. Click **Save**.

## Deleting an access profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **Edit** or click **View > Edit**.
4. In the **Access Profile** section, select the access profile that you want to delete and click **Delete**.

#### **Note:**

You cannot delete the Trust Management access profile.

## Creating a new port

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, perform one of the following steps:
  - Click **New**.
  - If you want to configure a port for an existing application instance, click an instance and then click **Edit** or click **View > Edit**.
4. Click **New** in the Port section.

5. Enter the information about the port in the following mandatory fields: **Name**, **Protocol**, and **Port**.
6. Click **Save**.

### Result

The table in the Port Details section displays the new port.

## Modifying a port

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. To configure a port for an existing element, perform one of the following steps on the Manage Elements page:
  - Select an element and click **Edit**.
  - Select an element and click **View > Edit**.
4. Click **Edit** in the **Port** section.
5. Modify the port information in the following fields: **Name**, **Port**, **Protocol**, and **Description**.
6. Click **Save** to save the changes to the database.

## Deleting a port

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select the application instance and click **Edit** or click **View > Edit**.
4. In the Port section, select the port you want to delete and click **Delete**.

The system deletes the port you selected from the table in the Port section.

---

## Managing and unmanaging elements from System Manager

### Manage elements

In a Geographic Redundancy-enabled system, the administrator can select elements and click **Manage** for the current System Manager to manage the elements. The system sends a notification to the element whose manageability status you must change. On receiving the notification, the element switches to the specific System Manager server from where you performed the Manage operation.

**\* Note:**

Session Manager from Release 6.3 and Communication Manager support the Manage operation.

During the split network, the administrator must ensure that the primary or the secondary System Manager server manages an element at a time, and not both systems.

**\* Note:**

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

**Related links**

[Manage Elements field descriptions](#) on page 933

## Unmanage elements

In a Geographic Redundancy-enabled system, the administrator can select to unmanage an element. The system sends a notification to the element whose manageability status you must change. On receiving the notification, the element unmanages from the current System Manager.

Communication Manager supports the Unmanage operation.

In a specific split network scenario, the primary System Manager server fails to communicate with the secondary System Manager server, but the element can communicate with both System Manager systems. If the primary System Manager server manages the element and the administrator wants to manage the element from the secondary System Manager server, on the primary System Manager server, the administrator must set the manageability status to Unmanaged.

**\* Note:**

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

**Related links**

[Manage Elements field descriptions](#) on page 933

---

# Adding Platform type elements to System Manager

---

## Adding System Platform to System Manager

### About this task

Use the procedure to manually add System Platform to System Manager. You can also use the System Manager discovery operation to discover System Platform in the network.

## Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in the **Type** field, click **System Platform**.

The page displays the On the New System Platform page.

5. On the General tab, provide the following information:
  - **Name**: The console domain (C-Dom) name.
  - **Type**: System Platform. A read-only field. The application type that the system populates from the **Type** field on the New Elements page.
  - **Description**: A description of the C-Dom.
  - **Node**: The IP address of C-Dom.
  - **Device Type**: System Platform.
6. On the Attributes tab, provide the following information:
  - **Login**: The use name with administrator permissions.
  - **Password**: The password.
  - **Confirm Password**: The password that you reenter.
  - **Dom0 IP Address**: The Dom-0 IP address.
  - **Cdom Root Password**: The C-Dom root password. A mandatory field.
  - **Confirm Cdom Root Password**: The C-Dom root password that you reenter. A mandatory field.

 **Note:**

If you do not complete the **Cdom Root Password** and **Confirm Cdom Root Password** fields, the upgrade operation fails.

7. In the Access Profile section, click **New** and provide the access profile details.

 **Note:**

The root access password must be identical in System Manager and System Platform.

8. Click **Commit**.

On the Manage Elements page, the system displays the System Platform instance that you added.

---

# Adding Application type elements to System Manager

---

## Adding Utility Services to System Manager

### About this task

From Release 8.0, Utility Services is replaced by AVP Utilities.

For Release 7.x, Utility Services is a mandatory component of Appliance Virtualization Platform in the Avaya-appliance deployment offer.

When you first install Appliance Virtualization Platform, you must add Utility Services to Appliance Virtualization Platform before you add System Manager.

Use the procedure to manually add Utility Services to System Manager.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in **Type**, click **Utility Services**.

The system displays the New Utility Services page.

5. On the General tab, provide the following information:
  - **Name:** The Utility Services name.
  - **Type:** Utility Services, a read-only field. The application type that the system populates from the **Type** field on the New Elements page.
  - **Description:** A description of Utility Services.
  - **Node:** The IP address of Utility Services.
  - Complete the remaining required fields.

For more information, see “Element details field descriptions”.

6. Click **Commit**.

On the Manage Elements page, the system displays the Utility Services instance that you added.

### Related links

[Element details field descriptions](#) on page 936

---

## Adding a Communication Manager instance to System Manager

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in the **Type** field, click **Communication Manager**.

The system displays the Add Communication Manager page.

5. On the **General Attributes** tab, provide the following information:

- a. Enter the Communication Manager server name.

For Branch Session Manager upgrades, provide the survivable remote server name.

- b. Enter the host name or IP Address of the Communication Manager server.

The IP address can be in the IPv4 or IPv6 format.

 **Note:**

- For duplex Communication Manager, provide the IP address for the active Communication Manager server and the standby Communication Manager server address in **Alternate IP Address**.
  - In a duplex configuration, while adding a Communication Manager instance to System Manager, virtual address of Communication Manager must not be used as it is not supported.
- c. Enter the customer login name that is required to access Communication Manager.  
For Branch Session Manager upgrades, provide the customer login name required to access the survivable remote server.
  - d. Under **Authentication Type**, select the required option.
  - e. Enter and reenter the password, or ASG key required to access Communication Manager.
  - f. Enter the port number of the Communication Manager server.
  - g. To view the Communication Manager system in the list, ensure that the **Add to Communication Manager** check box is selected.
  - h. In **CM Array Type**, click **Non-Array** to add as non cluster Communication Manager.

 **Important:**

If you are deploying Communication Manager by using Solution Deployment Manager, you must set the array type after deployment.



6. On the **SNMP Attributes** tab, perform the following:
  - a. Under **Version**, select **V1**.
  - b. Enter the required information.
  - c. From **Device Type**, select the type of Communication Manager.
7. Click **Commit**.

The system displays the Communication Manager instance that you added on the Manage Elements page.

#### Related links

[Add Communication Manager field descriptions](#) on page 947

---

## Adding a Session Manager instance to System Manager

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click **Session Manager**.
5. Select **Core Session Manager** and click **Continue**.
6. In the General section, enter the following information:
  - a. In the **SIP Entity Name** field, enter the name of Session Manager.
  - b. In the **Description** field, add a description for this entity. This field is optional.
  - c. In the **Management Access Point Host Name/IP** field, enter the IP address of the management interface of the Session Manager server.
  - d. **Maintenance Mode** is enabled by default. Clear the **Maintenance Mode** check box if you are not:
    - Staging a non-operational Session Manager or Branch Session Manager.
    - Pre-administering a Session Manager or Branch Session Manager on System Manager before the host installation.
7. Enter or select the appropriate information in the remaining required fields.  
For more information, see “Element details field descriptions”.
8. Click **Commit**.

#### Related links

[Element details field descriptions](#) on page 936

---

## Adding an Application Enablement Services instance to System Manager

### About this task

Use the following procedure if you are migrating or deploying using SDM, or if you are connecting Presence Services server to the AE Services server using the Presence Service connector.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Click **New**.
4. On the New Elements page, in the **Type** field, click **Application Enablement Services**.
5. In the General section, do the following:
  - a. In the **Name** field, type the name of the application.
  - b. In the **Description** field, add a description for this entity.  
This field is optional.
  - c. In the **Node** field, type the IP address of the management interface of the AE Services server.
6. In the remaining required fields, enter the appropriate information.  
For more information, see “Element details field descriptions”.
7. Click **Commit**.

### Related links

[Adding an Application Enablement Services instance to System Manager field descriptions](#) on page 951

---

## Adding G430 or G450 Branch Gateway to System Manager

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.
4. On the New Elements page, in **Type**, click **Media Gateways**.
5. On the New Media Gateway page, do the following:
  - a. In **Name**, type the name.

- b. In **Device Type**, click **Avaya G430** or **Avaya G450**.
  - c. In **Access Profile**, configure the parameters.
  - d. In **Port**, configure the parameters.
6. On **Attributes** and **Assign Elements** tabs, provide the required details.

For more information, see “Element details field descriptions”.

 **Note:**

The following parameters must be identical in System Manager and G430 Branch Gateway or G450 Branch Gateway:

- The root access password
- The SNMPv1 credentials

7. Click **Commit**.

On the **Manage Elements** page, the system displays the gateway that you added.

### Related links

[Element details field descriptions](#) on page 936

---

## Adding an Avaya Messaging profile for a user

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the **Manage Elements** page, click **New**.
4. On the **New Elements** page, in **Type**, click **Officelinx**.
5. On the **General** tab, in the **Node** field, type the IP address or FQDN according to the configuration in the actual Avaya Messaging server.

System Manager uses these details to establish communication between System Manager and Avaya Messaging.

6. On the **Attributes** tab, provide the Avaya Messaging login name and password.
7. Click **Commit**.

The system adds Avaya Messaging in System Manager.

8. On the **Manage Elements** page, click **System Manager**, and click **More Actions > Manage Trusted Certificates**.
9. On the **Manage Trusted Certificates** page, click **Add** to add a trusted certificate for the Avaya Messaging server.

For information about adding trusted certificates, see “Adding trusted certificate”.

For information about Avaya Messaging, see Avaya Avaya Messaging documentation on the Avaya Support website.

## Related links

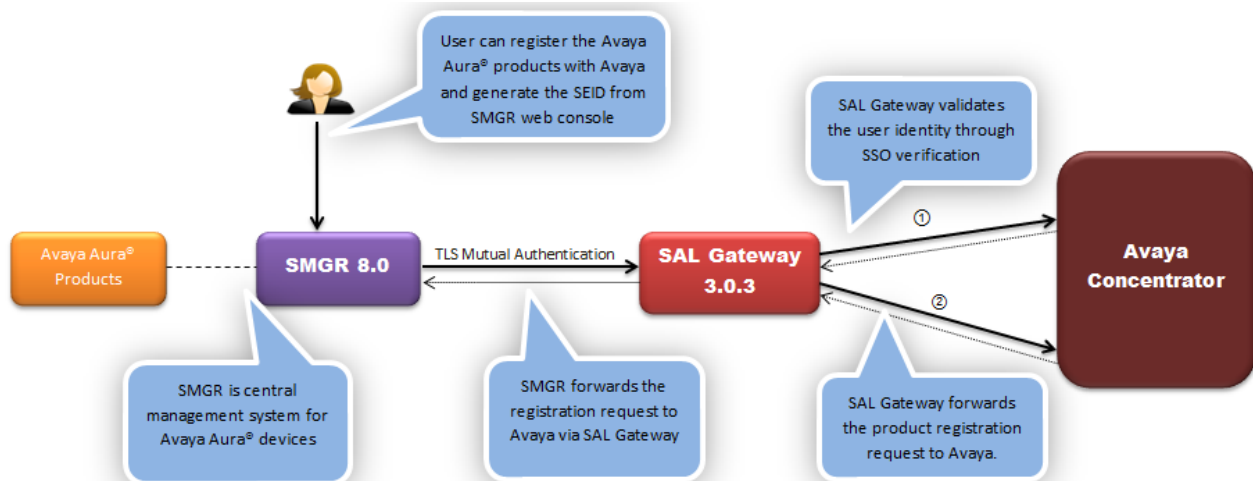
[Element details field descriptions](#) on page 936

# Product Initiated Registration overview

With System Manager Release 8.0, you can register the Avaya Aura® products from the System Manager web console to make the products serviceability ready.

You can use the Manage Elements page of System Manager to configure the SAL gateway and register the product. After the product is registered, the system generates an SEID and you can view the registration status in the **Reg.Status** column on the Manage Elements page.

The following diagram depicts the product registration with System Manager and SAL Gateway:



For information about the:

- SAL gateway and the Product Initiated Registration feature, see *Administering Avaya Diagnostic Server SAL Gateway* on the Avaya Support website.
- Products that support the Product Initiated Registration feature through the System Manager web console, see *Secure Access Link Supported Products* on the Avaya Support website.

## Configuring SAL Gateway

### About this task

You can configure only one SAL gateway for a given System Manager application.

## Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, click **More Actions > SAL Gateway configuration**.

The system displays the SAL Gateway configuration page.

3. In **SAL Gateway Name**, type a generic name of the SAL gateway.
4. In **SAL Gateway Address**, type the FQDN or IP Address of the SAL gateway.
5. In **SAL Gateway Port**, type the port number of the SAL gateway.

The default port is 7443.

6. In **Max Elements per request**, type the number of elements that you want to register to the SAL gateway.

The maximum number of elements is 10.

7. In **Request timeout in minutes**, type the number of minutes after which the request times out.

The maximum number of minutes is 90, which is the default value. The minimum number of minutes is 30.

8. To import the SAL gateway certificate, click one of the following:

- **Import Certificate.**
- **Services > Inventory > More Actions > Manager Trusted Certificates**

9. To check the SAL gateway connectivity, click **Test Connection**.

10. Click **Commit** to save the changes.

The system displays the message: SAL Gateway Configuration successful.

---

## Configuring Avaya Services registration

### About this task

Use this procedure to register Avaya products with SAL Gateway.

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select one or more element.

You can select up to 10 elements or the number of elements configured in the **Max Elements per request** field.

3. On the Manage Elements page, click **More Actions > Avaya Services Registration**.

The system displays the Product Registration page.

4. To validate the user identity and authenticate the user, in **SSO User Name**, type the SSO user name registered with Avaya.

An SSO user must have permission to register products against the supplied **FL/Sold To** number.

5. To validate the user identity and authenticate the user, in **SSO User Password**, type the password of the SSO user.

The system does not store the password.

6. In **FL/Sold To**, type the Functional Location number of the element.

The Functional Location number must be of 10 digits.

7. Click **Commit** to save the changes.

The system displays the registration status in the **Reg.Status** column on the Manage Elements page.

---

## Viewing notification status

### About this task

Use this procedure to view the notification status of the elements.

**View Notification Status** is available only on the primary or the secondary System Manager server that is in the active state.

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, click **More Actions > View Notification Status**.

System Manager displays the View Notification Status page with **Name**, **Event Type**, **Status**, **Last Updated Time**, and **Error**.

3. To resend the notification status, in the Notification Status section, select an event name, and click **Resend Notification**.

If the notification status is **Inprogress**, use **Get Current Status** to find the connectivity status and the manageability status of elements. However, you cannot use **Manage** or **Unmanage** to start or stop managing the elements.

If there is ongoing notification being sent in the background, the system displays a progress bar and removes the progress bar once the sending operation is complete or fails.

## Viewing certificate add status of elements

### About this task

When you add trusted certificates for:

- Multiple elements of same ElementType and Version, the system creates a job and you can view the certificate management job status.
- Single element, the system does not create a job.

Use this procedure to view the certificate management job status of the failed elements.

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, click **More Actions > View Certificate Add Status**.

System Manager displays the Certificate Management Jobs page with **Job Name**, **Job State**, **Total Elements**, **Failed Elements**, **Job Start Time**, and **Job End Time**.

3. To view the details, in the Certificate Management Job Status section, select a job name, and click **View**.

System Manager displays the Failed Elements Detail For Job - <Job\_Name> section with **Element IP**, and **Error Message**.

4. Click **Close** to close the Failed Elements Detail For Job - <Job\_Name> section.
5. Click **Back** to return to the Manage Elements page.

## Field descriptions

### Manage Elements field descriptions

| Name        | Description                                                                                                                                                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b> | The name of the element.                                                                                                                                                                                                                                                       |
| <b>Node</b> | The node on which the element runs. The IP address can be in the IPv4 or IPv6 format.                                                                                                                                                                                          |
| <b>Type</b> | <p>The type of the element to which the element belongs.</p> <p> <b>Note:</b></p> <p>You can view this field only if you gain access to the Manage Elements page from <b>Inventory</b>.</p> |

*Table continues...*

| Name               | Description                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Device Type</b> | The device type of the element.<br>For example, for IP Office, the device type can be IP Office or B5800. |
| <b>SEID</b>        | The number is generated after product registration for further configuration and investigation.           |
| <b>Reg. Status</b> | The registration status of the element with the SAL gateway.                                              |

The system also provides the following fields when System Manager is configured with Geographic Redundancy.

| Name                     | Description                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reachable</b>         | The state that specifies if the element is reachable from the current server. The values are Yes and No.                                                                                     |
| <b>Managed by</b>        | The server that manages this element. The options are Primary and Secondary. For a non-GR element, the field displays Not Supported.                                                         |
| <b>Last Updated Time</b> | The time when the system updates the status of the element.                                                                                                                                  |
| <b>Error</b>             | A red cross icon (  ) if the system generates errors. For more information, you can click the icon.         |
| <b>Warning</b>           | A yellow triangle icon (  ) if the system generates warnings. For more information, you can click the icon. |

 **Note:**

At any given point of time, you can perform **Get Current Status**, **Manage**, or **Unmanage** operation.

| Button         | Description                                                                              |
|----------------|------------------------------------------------------------------------------------------|
| <b>View</b>    | The View <Element-name> page. Use this page to view the details of the selected element. |
| <b>Edit</b>    | The Edit <Element-name> page. Use this page to modify the information of the instance.   |
| <b>New</b>     | The New Elements page. Use this page to create a new element.                            |
| <b>Delete</b>  | The Delete <Element-name> page. Use this page to delete a selected element.              |
| <b>Details</b> | The Element Details page. Use this page to view the details of the selected element.     |

*Table continues...*



| Button                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Get Current Status</b>                             | <p>The real-time connectivity status and the manageability status of elements on the active server.</p> <p>When the request is in progress for at least one element, the system displays the progress bar and the selected elements. When the request is complete, the system updates the time stamp and the status.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>On the secondary System Manager server in the standby mode, the system displays only the connectivity status of elements and not the manageability status.</li> <li>On a standalone server, the system disables <b>Get Current Status</b>.</li> </ul>                                                                                                                                                               |
| <b>More Actions &gt; Manage Trusted Certificates</b>  | The Trusted Certificates page. Use this page to view, add, export, and delete the trusted certificates for the element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>More Actions &gt; Manage Identity Certificates</b> | The Identity Certificates page. Use this page to view, export, renew, and replace the identity certificates for the element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>More Actions &gt; Manage</b>                       | An option to set System Manager to start managing the selected element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>More Actions &gt; Unmanage</b>                     | An option to set System Manager to stop managing the selected element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>More Actions &gt; Import</b>                       | The Import Applications page. Use this page to import application data in bulk from a valid XML file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>More Actions &gt; View Notification Status</b>     | <p>The status of notifications. If a notification is pending, the system displays the progress bar.</p> <p>The system displays the <b>Resend Notification</b> button only when there are no notifications in progress and when you select the rows of the same event type.</p> <p>The valid statuses are <b>Completed</b>, <b>Failed</b>, and <b>Inprogress</b>.</p> <p>If the notification status is <b>Inprogress</b>, use <b>Get Current Status</b> to find the connectivity status and the manageability status of elements. However, you cannot use <b>Manage</b> or <b>Unmanage</b> to start or stop managing the elements.</p> <p> <b>Note:</b></p> <p><b>View Notification Status</b> is available only on the primary or the secondary System Manager server that is in the active state.</p> |
| <b>More Actions &gt; View Certificate Add Status</b>  | The Certificate Management Jobs page. Use this page to view the certificate status of elements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>More Actions &gt; SAL Gateway configuration</b>    | The SAL Gateway configuration page. Use this page to configure the SAL gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>More Actions &gt; Product Registration</b>         | The Product Registration page. Use this page to register the Avaya products with SAL Gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Advanced Search</b>                                | The link to perform advance search. When you click on this link, System Manager displays the Criteria section.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table continues...

| Button                 | Description                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------|
| <b>Filter: Enable</b>  | The fields where you can set the filter criteria. <b>Filter: Enable</b> is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields. <b>Filter: Disable</b> is a toggle button.                  |
| <b>Filter: Apply</b>   | Filters elements based on the filter criteria.                                              |
| <b>Select: All</b>     | Selects all elements in the table.                                                          |
| <b>Select: None</b>    | Clears the selection for the users that you select.                                         |
| <b>Refresh</b>         | Refreshes the element information in the table.                                             |

## Criteria

| Name                          | Description                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Search Criteria</b> | The options are: <ul style="list-style-type: none"> <li>• <b>Replica Node Host Name</b></li> <li>• <b>Synchronization State</b></li> <li>• <b>Last Synchronization Time</b></li> </ul>               |
| <b>Select Search Operator</b> | The options are: <ul style="list-style-type: none"> <li>• <b>Equals</b></li> <li>• <b>Not Equals</b></li> <li>• <b>Starts with</b></li> <li>• <b>Ends with</b></li> <li>• <b>Contains</b></li> </ul> |
| <b>Enter Search to Text</b>   | Specify the search criteria.                                                                                                                                                                         |

| Button        | Description                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| -             | Removes the additional search criteria fields.<br>This field is enabled when the additional search criteria fields are added. |
| +             | Adds the additional search criteria fields.                                                                                   |
| <b>Clear</b>  | Clears the search criteria.                                                                                                   |
| <b>Search</b> | Performs the search for the specified search criteria                                                                         |
| <b>Close</b>  | Closes the Criteria section.                                                                                                  |

## Element details field descriptions

### **Note:**

The fields on this page varies with the application that you manage.

## General

| Name | Description                                             |
|------|---------------------------------------------------------|
| Type | The application type whose instance you want to create. |

The following field is available only for specific applications, such as Session Manager and Presence Services.

| Name                                     | Description                                                                                                                                                                                  |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select type of <application name> to add | The application type whose instance you want to create.<br>For example, for Presence Services, you can select a standalone Presence Services or Presence Services on Avaya Breeze® platform. |

| Name        | Description                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | The name of the element.                                                                                                                                                                                                                                                                             |
| Type        | The type of the application to which the element belongs.                                                                                                                                                                                                                                            |
| Description | A brief description of the element.                                                                                                                                                                                                                                                                  |
| Node        | The node on which you run the element. The IP address can be in the IPv4 or IPv6 format.<br><br> <b>Note:</b><br>The system displays the <b>Node</b> field when you select <b>Other</b> from the <b>Node</b> field. |
| Device Type | The device type of the element.<br>For example, for IP Office, the device type can be IP Office or B5800.                                                                                                                                                                                            |

## Access Profile

| Name                | Description                                                                                                                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                | The name of the access profile.                                                                                                                                                                                                                           |
| Access Profile Type | The type of the access profile. The options are: <ul style="list-style-type: none"> <li>• <b>URI</b>: For system web services API.</li> <li>• <b>SSH</b>: For application upgrade functions.</li> <li>• <b>SNMP</b>: For discovering elements.</li> </ul> |

*Table continues...*

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access Profile Sub Type</b> | The sub type of the URI access profile. The options are: <ul style="list-style-type: none"> <li>• <b>EMURL</b>: To create a URL type access profile.</li> <li>• <b>WS</b>: To create a web service access profile.</li> <li>• <b>GUI</b>: To create a GUI access profile.</li> <li>• <b>GRCommunication</b>: To create a GR-aware element.</li> <li>• <b>TenantURL</b>: To create the tenant-related access profile.</li> <li>• <b>Other</b></li> </ul> |
| <b>Protocol</b>                | The protocol that the element supports to communicate with other communication devices.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Host</b>                    | The name of the host on which the element is running.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Port</b>                    | The port on which the element is running.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Order</b>                   | The order in which you gain access to access profiles.                                                                                                                                                                                                                                                                                                                                                                                                  |

| Button        | Description                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View</b>   | Displays fields in the Access Profile section that you can use to view access profile details.                                                         |
| <b>New</b>    | Displays the Application System Supported Protocol and Access Profile Details subsections in the Access Profile section to add access profile details. |
| <b>Edit</b>   | Displays fields in the Access Profile section using which you can modify the access profile details that you select.                                   |
| <b>Delete</b> | Deletes the selected access profile.                                                                                                                   |

### Application System Supported Protocol

The system displays the following fields when you click **New** or **Edit** in the **Access Profile** section:

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol</b> | The protocol used to access profiles. The options are: <ul style="list-style-type: none"> <li>• <b>URI</b>: For system web services API.</li> <li>• <b>SSH</b>: For application upgrade functions.</li> <li>• <b>SNMP</b>: For discovering elements.</li> </ul> <p> <b>Note:</b></p> <p>The page displays the button only when you click <b>Add</b> or <b>Edit</b> in the Access Profile section.</p> |

### Access Profile Details

The page displays the following fields when you click **URI** in the **Protocol** field:

| Name                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                | The name of the access profile.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Access Profile Type</b> | The type of the access profile. The options are: <ul style="list-style-type: none"> <li>• <b>EMURL</b>: To create a URL type access profile.</li> <li>• <b>WS</b>: To create a web service access profile.</li> <li>• <b>GUI</b>: To create a GUI access profile.</li> <li>• <b>GRCommunication</b>: To create a GR-aware element.</li> <li>• <b>TenantURL</b>: To create the tenant-related access profile.</li> <li>• <b>Other</b></li> </ul> |
| <b>Protocol</b>            | The protocol for communicating the element.                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Host</b>                | The name of the host on which the element is running.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Port</b>                | The port on which the element is running.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Path</b>                | The path to gain access to the access profile.                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Order</b>               | The order in which you gain access to access profiles.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>         | A brief description of the access profile.                                                                                                                                                                                                                                                                                                                                                                                                      |

The page displays the following fields when you click **SSH** in the **Protocol** field:

| Name                    | Description                                  |
|-------------------------|----------------------------------------------|
| <b>Name</b>             | The name of the access profile.              |
| <b>Login Name</b>       | The login name as configured on the element. |
| <b>Port</b>             | The port on which the element is running.    |
| <b>Password</b>         | The password to log in to the element.       |
| <b>Confirm Password</b> | The password that you retype.                |

The page displays the fields when you click **SNMP** in the **Protocol** field and **V3** in the **Type** field:

| Name                | Description                              |
|---------------------|------------------------------------------|
| <b>Profile Name</b> | The name of the profile.                 |
| <b>Description</b>  | A brief description of the profile.      |
| <b>Type</b>         | The SNMP protocol type.                  |
| <b>User</b>         | The user name as defined in the element. |

*Table continues...*

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Type</b>             | <p>The authentication protocol used to authenticate the source of traffic from SNMP V3 users. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>MD5</b></li> </ul> <p>The default is <b>MD5</b>.</p> <ul style="list-style-type: none"> <li>• <b>SHA</b></li> <li>• <b>None</b></li> </ul> <p><b>Authorization Type</b> applies only to the SNMP V3 protocol.</p>                                                                                                  |
| <b>Authentication Password</b>         | <p>The password to authenticate the user. The password must contain at least eight characters.</p> <p> <b>Note:</b></p> <p>The password is mandatory.</p>                                                                                                                                                                                                                                                |
| <b>Confirm Authentication Password</b> | The SNMP V3 protocol authentication password that you retype for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Privacy Type</b>                    | <p>The encryption policy for an SNMP V3 user. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>AES</b>: For SNMP-based communication.</li> <li>• <b>AES128</b>: For SNMP-based communication.</li> <li>• <b>DES</b>: For SNMP-based communication.</li> </ul> <p>The default is <b>DES</b>.</p> <ul style="list-style-type: none"> <li>• <b>None</b>: Does not encrypt traffic for this user.</li> </ul> <p>Set <b>Privacy Type</b> only for an SNMP V3 user.</p> |
| <b>Privacy Password</b>                | The password used to enable the <b>DES</b> or <b>AES</b> encryption. DES passwords must contain at least eight characters.                                                                                                                                                                                                                                                                                                                                                                |
| <b>Confirm Privacy Password</b>        | The privacy password that you retype for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Privileges</b>                      | <p>The privileges that determine the operations that you can perform on MIBs.</p> <ul style="list-style-type: none"> <li>• <b>None</b></li> </ul> <p>The default is None.</p> <ul style="list-style-type: none"> <li>• <b>Read/Write</b>: To perform GET and SET operations.</li> <li>• <b>Read</b>: To perform only the GET operation.</li> </ul>                                                                                                                                        |
| <b>Timeout</b>                         | The time in milliseconds for which the element waits for a response from the device being polled during discovery.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Retries</b>                         | The number of times that the element polls a device without receiving a response before timing out.                                                                                                                                                                                                                                                                                                                                                                                       |

The page displays the fields when you click **SNMP** in the **Protocol** field and **V1** in the **Type** field:

| Name                   | Description                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>    | The name of the profile.                                                                                                       |
| <b>Description</b>     | A brief description of the profile.                                                                                            |
| <b>Type</b>            | The SNMP protocol type.<br><br>* <b>Note:</b><br>To upgrade Communication Manager using SNMP protocol, you must select SNMPV1. |
| <b>Read Community</b>  | The read community of the device.<br><b>Read Community</b> applies only to the SNMP V1 protocol.                               |
| <b>Write Community</b> | The write community of the device.<br><b>Write Community</b> applies only to the SNMP V1 protocol.                             |
| <b>Timeout</b>         | The time in milliseconds for which the element waits for a response from the device that the element polls.                    |
| <b>Retries</b>         | The number of times that the element polls a device and fails to receive a response. After the retries, the element times out. |

| Button        | Description                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Save</b>   | Saves the access profile details.<br><br>* <b>Note:</b><br>This button is available only when you click <b>Add</b> and <b>Edit</b> in the Access Profile section.                                                                                                             |
| <b>Cancel</b> | Cancels the operation of creating or editing an access profile and hides the fields where you enter or modify the access profile information.<br><br>* <b>Note:</b><br>This button is available only when you click <b>Add</b> and <b>Edit</b> in the Access Profile section. |

## Port

| Name               | Description                               |
|--------------------|-------------------------------------------|
| <b>Name</b>        | The name of the port.                     |
| <b>Port</b>        | The port on which the element is running. |
| <b>Protocol</b>    | The protocol for the corresponding port.  |
| <b>Description</b> | A brief description about the port.       |

| Button      | Description                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------|
| <b>New</b>  | Displays fields in the Port section that you can use to add a port.                                          |
| <b>Edit</b> | Displays fields in the Port section with port information. You can change the port details in the port mode. |

*Table continues...*

| Button        | Description                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Delete</b> | Deletes the selected configured port.                                                                                                                                                                                                                                               |
| <b>Commit</b> | Saves the port details.<br><br>* <b>Note:</b><br>The section displays the <b>Save</b> button only when you click <b>Add</b> or <b>Edit</b> in the Port section.                                                                                                                     |
| <b>Cancel</b> | Cancels the current operation of creating or editing an access profile and hides the fields where you add or modify the port information.<br><br>* <b>Note:</b><br>The section displays the <b>Cancel</b> button only when you click <b>Add</b> or <b>Edit</b> in the Port section. |

## Attributes

Use this section to configure attributes for the selected element.

The following fields display the information about attributes defined for System Manager.

| Name                | Description                                                    |
|---------------------|----------------------------------------------------------------|
| <b>IP</b>           | The IP address of System Manager.                              |
| <b>FQDN</b>         | FQDN of System Manager.                                        |
| <b>Virtual IP</b>   | The virtual IP address of System Manager.                      |
| <b>Virtual FQDN</b> | The virtual FQDN of System Manager.                            |
| <b>isPrimary</b>    | The option to indicate if the element is primary or secondary. |

## Assign elements

| Name               | Description                                               |
|--------------------|-----------------------------------------------------------|
| <b>Name</b>        | The name of the element.                                  |
| <b>Type</b>        | The type of the application to which the element belongs. |
| <b>Description</b> | A brief description about the element.                    |

| Button                   | Description                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------|
| <b>Assign elements</b>   | Displays the Assign elements page that you use to assign an element to another element. |
| <b>Unassign elements</b> | Removes an assigned element.                                                            |



| Button        | Description                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Creates or modifies an element by saving the information to the database.<br><br>* <b>Note:</b><br>The system displays the button only when you click <b>Add</b> or <b>Edit</b> on the Manage Elements page. |
| <b>Cancel</b> | Closes the page without saving the information and navigates back to the Manage Elements page.                                                                                                               |

For example, the following fields provide information about attributes that you can define for Messaging.

| Name                           | Description                                                                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Login</b>                   | The name in the <b>Trusted Server Name</b> field of the Trusted Servers page on the Messaging server.                                                                                                                                                               |
| <b>Password</b>                | The password as given in the <b>Password</b> field of the Trusted Servers page on the Messaging server.                                                                                                                                                             |
| <b>Confirm Password</b>        | The password that you retype for confirmation.                                                                                                                                                                                                                      |
| <b>Messaging Type</b>          | The type of the Messaging server. The following types are supported: <ul style="list-style-type: none"> <li>• <b>MM</b>: Modular Messaging</li> <li>• <b>CMM</b>: Communication Manager Messaging</li> <li>• <b>AURAMESSAGING</b>: Avaya Aura® Messaging</li> </ul> |
| <b>Version</b>                 | The version of Messaging. Supported versions are 5.0 and later.                                                                                                                                                                                                     |
| <b>Secured LDAP Connection</b> | An option to use the secure LDAP connection.<br>To use the nonsecure LDAP connection, you must clear the check box.                                                                                                                                                 |
| <b>Port</b>                    | The port on which the LDAP or secure LDAP service that the element provides is running. The default port is 389 for LDAP and 636 for secure LDAP.                                                                                                                   |
| <b>Location</b>                | The location of the element.                                                                                                                                                                                                                                        |

## Delete Element Confirmation field descriptions

Use this page to delete an element.

| Name        | Description                                                                                 |
|-------------|---------------------------------------------------------------------------------------------|
| <b>Name</b> | The name of the element.                                                                    |
| <b>Node</b> | The node on which the element is running. The IP address can be in the IPv4 or IPv6 format. |

*Table continues...*

| Name                | Description                                                                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Registration</b> | The registration status of the element. The options are: <ul style="list-style-type: none"> <li>• <b>True:</b> Indicates a registered instance.</li> <li>• <b>False:</b> Indicates an unregistered instance.</li> </ul> |
| <b>Description</b>  | A brief description about the element.                                                                                                                                                                                  |

| Button        | Description                                  |
|---------------|----------------------------------------------|
| <b>Delete</b> | Deletes the selected element.                |
| <b>Cancel</b> | Closes the Delete Element Confirmation page. |

## Import Elements field descriptions

Use this page to import element data in bulk from a valid XML file.

### File Selection

| Name               | Description                                                                    |
|--------------------|--------------------------------------------------------------------------------|
| <b>Select File</b> | The path and name of the XML file from which you must import the element data. |

| Button        | Description                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------|
| <b>Browse</b> | Displays the File Upload box where you can browse for the file that you must import the element data. |

### Configuration

| Name                              | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Error Configuration</b> | The options are: <ul style="list-style-type: none"> <li>• <b>Abort on First Error:</b> The system stops the import of element data when the import element operation encounters the first error in the import file that contains the element data.</li> <li>• <b>Continue Processing other records:</b> The system imports the data of next element if the data of current element failed to import.</li> </ul> |

*Table continues...*

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>If a matching record already exists</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Skip:</b> Skips a matching record that already exists in the system during an import operation.</li> <li>• <b>Replace:</b> Reimports or replaces all the data for an element. This is essentially the ability to replace an element along with the other data related to the element.</li> <li>• <b>Merge:</b> Imports the element data at an even greater degree of granularity. Using this option you can simultaneously perform both the add and update operation of elements data.</li> <li>• <b>Delete:</b> Deletes the elements along with their data from the database that match the records in the input XML file.</li> </ul> |

## Schedule

| Name                | Description                                                                                                                                                                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Job</b> | <p>The options for configuring the schedule of the job:</p> <ul style="list-style-type: none"> <li>• <b>Run immediately:</b> Use this option if you want to run the import job immediately.</li> <li>• <b>Schedule later:</b> Use this option to run the job at the specified date and time.</li> </ul> |
| <b>Date</b>         | <p>The date when you require to run the import elements job. The date format is mm: dd:yyyy. You can use the calendar icon to select a date.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                  |
| <b>Time</b>         | <p>Time of running the import elements job. The time format is hh:mm:ss and 12 (AM or PM) or 24 hour format.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                                  |
| <b>Time Zone</b>    | <p>Time zone of your region.</p> <p>This field is available when you select the <b>Schedule later</b> option for scheduling a job.</p>                                                                                                                                                                  |

| Button        | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| <b>Import</b> | Imports or schedules the import operation based on the option you selected. |

## Import List

| Name                    | Description                              |
|-------------------------|------------------------------------------|
| <b>Select check box</b> | Provides the option to select a job.     |
| <b>Start Time</b>       | The time and date of scheduling the job. |

*Table continues...*

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Status</b>          | The current status of the job. The following are the different status of the job: <ol style="list-style-type: none"> <li>1. PENDING EXECUTION: The job is in queue.</li> <li>2. RUNNING: The job execution is in progress.</li> <li>3. SUCCESSFUL: The job execution is complete.</li> <li>4. INTERRUPTED: The job execution is cancelled.</li> <li>5. PARTIAL FAILURE: The job execution has partially failed.</li> <li>6. FAILED: The job execution has failed.</li> </ol> |
| <b>Scheduled Job</b>   | Displays a link to the Scheduler user interface. You can cancel the job from the Scheduler user interface too.                                                                                                                                                                                                                                                                                                                                                               |
| <b>% Complete</b>      | The job completion status in percentage.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Element Records</b> | The number of user records in the input file.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Failed Records</b>  | The number of user records in the input file that failed to import.                                                                                                                                                                                                                                                                                                                                                                                                          |

| Button              | Description                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Job</b>     | Shows the details of the selected job.                                                                                                                                   |
| <b>Cancel Job</b>   | Cancels the import operation for the selected job. You can cancel a job that is in progress or queued for import.                                                        |
| <b>Delete Job</b>   | Deletes the selected job.                                                                                                                                                |
| <b>Refresh</b>      | Refreshes the job information in the table.                                                                                                                              |
| <b>Show</b>         | Provides an option to view all jobs on the same page. If the table displaying scheduled jobs span multiple pages, to view all jobs on a single page, select <b>All</b> . |
| <b>Select: All</b>  | Selects all jobs in the table.                                                                                                                                           |
| <b>Select: None</b> | Clears the check box selections.                                                                                                                                         |
| <b>Cancel</b>       | Returns to the <b>Manage Elements</b> page.                                                                                                                              |

## Import Status field descriptions

The Import Status page displays the detailed status of the selected import job.

### Status Summary

| Name         | Description                                                      |
|--------------|------------------------------------------------------------------|
| <b>Start</b> | The start date and time of the job.                              |
| <b>End</b>   | The end date and time of the job.                                |
| <b>File</b>  | The name of the file that is used to import the element records. |

*Table continues...*

| Name                      | Description                                                         |
|---------------------------|---------------------------------------------------------------------|
| <b>Total Records</b>      | The total number of element records in the input file.              |
| <b>Successful Records</b> | The total number of element records that are successfully imported. |
| <b>Failed Records</b>     | The total number of element records that failed to import.          |
| <b>Complete</b>           | The percentage completion of the import.                            |

### Status Details

| Name                 | Description                                           |
|----------------------|-------------------------------------------------------|
| <b>Line Number</b>   | The line number in the file where the error occurred. |
| <b>loginName</b>     | The login name through which job was executed.        |
| <b>Error Message</b> | A brief description about the error message.          |

| Button      | Description                          |
|-------------|--------------------------------------|
| <b>Done</b> | Returns to the Import Elements page. |

## Add Communication Manager field descriptions

### General Attributes

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                   | The name of the Communication Manager instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hostname or IP Address</b> | The IP address can be in the IPv4 or IPv6 format. The host name or the IP address of the Communication Manager instance.<br><br>For the duplicated Communication Manager, this value references the active server IP address.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Alternate IP Address</b>   | The alternate IP address of the element. For duplex servers, the alternate IP address is the IP address of the standby server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Login</b>                  | The login name that you use to connect to the Communication Manager instance.<br><br> <b>Note:</b><br><br>craft, craft2, dadmin, inads, init, rasaccess, sroot, and tsc are the restricted logins when you configure a Communication Manager system.<br><br>Do not use the login name to connect to: <ul style="list-style-type: none"> <li>• The Communication Manager instance from any other application.</li> <li>• The Communication Manager SAT terminal by using command line interface (CLI).</li> </ul> |
| <b>Authentication Type</b>    | The authentication type for the SSH or Telnet login name on the element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

*Table continues...*

| Name                                      | Description                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Password</b>                           | The password that authenticates the SSH or Telnet login name on the element.                                                                                                                                                                                                                                                       |
| <b>Confirm Password</b>                   | <p>The password that you retype for confirmation.</p> <p> <b>Note:</b><br/><b>Confirm Password</b> must match <b>Password</b>.</p>                                                                                                                |
| <b>ASG Key</b>                            | <p>The ASG key that authenticates the SSH or Telnet login name on the element.</p> <p>This field is only available if <b>ASG Key</b> is selected in <b>Authentication Type</b>.</p>                                                                                                                                                |
| <b>Confirm ASG Key</b>                    | <p>The ASG key that you retype for confirmation.</p> <p>This field is only available if <b>ASG Key</b> is selected in <b>Authentication Type</b>.</p> <p> <b>Note:</b><br/><b>Confirm ASG key</b> must match <b>ASG key</b>.</p>                  |
| <b>SSH Connection</b>                     | <p>An option to use SSH for connecting to the element.</p> <p>By default, this check box is selected and the system uses SSH to connect to the element.</p> <p>If you clear the check box, the system uses Telnet to connect to the element.</p>                                                                                   |
| <b>RSA SSH Fingerprint (Primary IP)</b>   | <p>The RSA SSH key of the Communication Manager server.</p> <p>For duplex servers, the RSA SSH key is the key of the active server.</p> <p>You must include the prefix <code>SHA256:</code> before the RSA SSH Fingerprint.</p> <p>For example:</p> <p><code>SHA256:&lt;Eb4qM3YEWONzZoLlhgle1s2Ena0A8qhy1z1oWk7Nahs&gt;</code></p> |
| <b>RSA SSH Fingerprint (Alternate IP)</b> | <p>The RSA SSH key of the standby Communication Manager server. Use the RSA SSH key only for duplex servers.</p> <p>You must include the prefix <code>SHA256:</code> before the RSA SSH Fingerprint.</p> <p>For example:</p> <p><code>SHA256:&lt;Ena0A8qhy1z1oWk7NahsYEWONzEb4qM3ZoLlhgle1s2&gt;</code></p>                        |
| <b>Description</b>                        | A description of the Communication Manager server.                                                                                                                                                                                                                                                                                 |

*Table continues...*

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Notifications</b>         | <p>A real-time notification whenever an administrative change occurs in Communication Manager. For example, when you add or delete an extension from Communication Manager outside System Manager. The options are:</p> <ul style="list-style-type: none"> <li>• Selected: Enables the CM Notify sync feature for this Communication Manager instance.</li> <li>• Cleared: Disables the CM Notify sync feature for this Communication Manager instance.</li> </ul> <p>After you enable this feature, and register the System Manager IP address on Communication Manager, the system sends changes that are administered on Communication Manager to System Manager asynchronously.</p> <p> <b>Note:</b></p> <p>Communication Manager 6.2 or later supports this feature.</p> |
| <b>Port</b>                         | <p>The port on which the service provided by the element is running. The default SSH port is 5022.</p> <p> <b>Note:</b></p> <p>From Communication Manager Release 7.1 and later, the telnet port 5023 is disabled. If the telnet port is configured for the Communication Manager element, select the <b>SSH Connection</b> checkbox. When you select this checkbox, the system populates the default port value to 5022.</p>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Location</b>                     | The location of the element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Add to Communication Manager</b> | <p>An option to select Communication Manager that you want to view in the communication manager list.</p> <p>By default, <b>Add to Communication Manager</b> is selected.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## SNMPv1 Attributes

In the **Version** field, when you select **V1**, System Manager displays the following fields.

| Name                   | Description                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Version</b>         | The SNMP protocol type.                                                                                                                 |
| <b>Read Community</b>  | The read community of the device.                                                                                                       |
| <b>Write Community</b> | The write community of the device.                                                                                                      |
| <b>Retries</b>         | <p>The number of times an application polls a device without receiving a response before timing out.</p> <p>The default value is 3.</p> |

*Table continues...*

| Name                | Description                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Timeout (ms)</b> | The duration of time in milliseconds for which an application polls a device without receiving a response before timing out.<br><br>The default value is 5000 ms.                                                                                                                                                                                                |
| <b>Device Type</b>  | The Communication Manager application type. The options are: <ul style="list-style-type: none"> <li>• <b>Avaya Aura(R) Communication Manager SP</b> for Communication Manager 6.3.100 on System Platform.</li> <li>• <b>Avaya Aura(R) Communication Manager VE</b> for Virtualized Environment-based Communication Manager 6.3.100 and Release 8.1.3.</li> </ul> |

### SNMPv3 Attributes

In the **Version** field, when you select **V3**, System Manager displays the following fields.

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Version</b>                         | The SNMP protocol type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>User Name</b>                       | The user name as defined in the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Authentication Protocol</b>         | The authentication protocol that authenticates the source of traffic from SNMP V3 protocol users. The possible values are: <ul style="list-style-type: none"> <li>• <b>MD5</b><br/>This is the default option.</li> <li>• <b>SHA</b></li> <li>• <b>None</b>: If you select this option, System Manager does not display the <b>Authentication Password</b>, <b>Confirm Authentication Password</b>, and <b>Privacy Protocol</b> fields.</li> </ul>                                                                        |
| <b>Authentication Password</b>         | The SNMP authentication password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Confirm Authentication Password</b> | The SNMP authentication password that you retype for confirmation. <b>Authentication Password</b> and <b>Confirm Authentication Password</b> must match.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Privacy Protocol</b>                | The encryption policy for SNMP V3 protocol users. The possible values are: <ul style="list-style-type: none"> <li>• <b>AES128</b>: Use the AES encryption for the SNMP-based communication. This is the default protocol.</li> <li>• <b>DES</b>: Use the DES encryption for the SNMP-based communication.</li> <li>• <b>None</b>: Does not encrypt traffic for this user.</li> </ul> If you select this option, System Manager does not display the <b>Privacy Password</b> , and <b>Confirm Privacy Password</b> fields. |
| <b>Privacy Password</b>                | The pass phrase used to encrypt the SNMP data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Confirm Privacy Password</b>        | Retype the privacy password in this field for confirmation.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

*Table continues...*



| Name                | Description                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Retries</b>      | The number of times the application polls a device without receiving a response before timing out.<br>The default value is 3.                        |
| <b>Timeout (ms)</b> | The duration of time in milliseconds for which the application waits for the response from the device being polled.<br>The default value is 5000 ms. |
| <b>Device Type</b>  | The type of device.                                                                                                                                  |

| Button        | Description                                             |
|---------------|---------------------------------------------------------|
| <b>Commit</b> | Adds a Communication Manager instance in the inventory. |
| <b>Clear</b>  | Clears all the entries.                                 |
| <b>Cancel</b> | Cancels your action and returns to the previous page.   |

## Adding an Application Enablement Services instance to System Manager field descriptions

### General

| Name               | Description                                                                      |
|--------------------|----------------------------------------------------------------------------------|
| <b>Name</b>        | The name of the Application Enablement Services instance.                        |
| <b>Type</b>        | The type of the instance added.<br>Application Enablement Services in this case. |
| <b>Description</b> | The description of the AE Services server.                                       |
| <b>Node</b>        | The IP address/FQDN of the management interface of the AE Services server.       |

### Port Details

| Name            | Description                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>     | The name of the port to be used for the AE Services server.                                                                                                                                                   |
| <b>Protocol</b> | The protocol type supported by the port and the AE Services server. The options are: <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> <li>• jnp</li> <li>• rmi</li> <li>• tsapi</li> </ul> |

*Table continues...*

| Name        | Description                                            |
|-------------|--------------------------------------------------------|
| Port        | The port number to be used for the AE Services server. |
| Description | The description of the port details.                   |

### Attributes

| Name                    | Description                             |
|-------------------------|-----------------------------------------|
| aes.aesMachineName.name | The hostname of the AE Services server. |

### Assign Elements

| Name            | Description                                                                                                                                                                                                                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assignment Name | The name to assign the Communication Manager instance to the AE Services server.<br><br> <b>Note:</b><br><b>Assignment Name</b> must be same as the Switch Connection name in the AE Services management console. |
| Name            | The name of the Communication Manager instance.                                                                                                                                                                                                                                                    |
| Node            | The IP address/FQDN of the management interface of the Communication Manager instance.                                                                                                                                                                                                             |
| Type            | The type of the Communication Manager instance.                                                                                                                                                                                                                                                    |
| Version         | The version number of the Communication Manager instance.                                                                                                                                                                                                                                          |

| Button | Description                                           |
|--------|-------------------------------------------------------|
| Commit | Adds a AE Services instance in the inventory.         |
| Save   | Saves all the entries.                                |
| Cancel | Cancels your action and returns to the previous page. |

### Related links

[Adding an Application Enablement Services instance to System Manager](#) on page 928

## Add IP Office field descriptions

### General

| Name        | Description                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | The name of the IP Office device. The name must only contain lowercase and uppercase alphabets, numbers from 0 to 9, commas, hyphens, and underscores. |
| Description | The description of the IP Office device.                                                                                                               |

*Table continues...*

| Name                            | Description                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Node</b>                     | The IP address can be in the IPv4 or IPv6 format. The host name or the IP address of the IP Office device. |
| <b>Device Type</b>              | The type of the IP Office device. The options are IP Office and B5800.                                     |
| <b>Device Version</b>           | The version of the IP Office device.                                                                       |
| <b>Service Login</b>            | The login name to access the IP Office device. The default is BranchAdmin.                                 |
| <b>Service Password</b>         | The password to access the IP Office device.                                                               |
| <b>Confirm Service Password</b> | The service password that you retype for confirmation.                                                     |

For IP Office releases earlier than 9.1, the default service login for IP Office is SMGRB5800Admin. After you upgrade IP Office from Release 9.0 to 9.1 or later, you can use the same login name, SMGRB5800Admin. The account remains active.

However, the system creates a new account, BranchAdmin. The configuration of the BranchAdmin account is the same as the SMGRB5800Admin account. The new account also becomes active.

In IP Office Release 9.1 or later, if you reset the security setting, the system deletes the SMGRB5800Admin account and adds the BranchAdmin account that remains disabled. You must activate the account by accessing the IP Office security setting offline.

Also, if you add the new IP Office Release 9.1 or later in System Manager by running Initial Configuration Utility (ICU) on IP Office, the default account, BranchAdmin, will be available. The account becomes active.

## SNMP

| Name                   | Description                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Version</b>         | The SNMP protocol type. The options are None and V1.                                                          |
| <b>Read Community</b>  | The read community of the device.                                                                             |
| <b>Write Community</b> | The write community of the device.                                                                            |
| <b>Retries</b>         | The number of times that an application polls a device without receiving a response before timing out.        |
| <b>Timeout (ms)</b>    | The number of milliseconds that an application polls a device without receiving a response before timing out. |

| Button        | Description                                                  |
|---------------|--------------------------------------------------------------|
| <b>Commit</b> | Adds the IP Office device to the inventory.                  |
| <b>Clear</b>  | Clears your entries and reset the page.                      |
| <b>Cancel</b> | Cancels the add operation, and returns to the previous page. |

---

## Delete IP Office field descriptions

| Name               | Description                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | The name of the IP Office instance you have chosen to delete.                                                                    |
| <b>Node</b>        | The node on which the IP Office instance you have chosen to delete is running. The IP address can be in the IPv4 or IPv6 format. |
| <b>Type</b>        | The type of the application instance you want to delete. In this case, <b>Type</b> is IP Office.                                 |
| <b>Version</b>     | The software version of the IP Office device you have chosen to delete.                                                          |
| <b>Description</b> | The description of the IP Office device you have chosen to delete.                                                               |

| Button        | Description                                                       |
|---------------|-------------------------------------------------------------------|
| <b>Delete</b> | Click to delete the IP Office device you have selected.           |
| <b>Cancel</b> | Click to cancel the delete operation and go to the previous page. |

---

## Managing Serviceability Agents

---

### Serviceability Agents

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and for alarming. The Serviceability Agent sends SNMPv2 and SNMPv3 traps and notifies the configured NMS destinations where System Manager and the SAL gateway are the two mandatory destinations.

With the Serviceability Agent user interface you can:

- Manage and configure SNMPv3 users remotely
- Manage and configure SNMP trap destinations remotely
- Create, edit, view, and delete user and target profiles. You can also attach these profiles to agents or detach these profiles from agents.

For more information on fault management using SNMP, see *Avaya Aura® System Manager Fault Management and monitoring using SNMP*.

## Converting a common alarm definition file to MIB file and trapd file

### Before you begin

To run the command, you require jre 1.6.0 or later installed on the system.

### About this task

The MIB tool converts a Common Alarm Definition File (CADF) xml file to MIB file (.my) and trapd (.conf) file. The tool converts only CADF files with notification OIDS that are specified in the X.X.X.productID.0.n format, where n is the notification OID.

You must provide all parameters. To provide the parameters later, you must edit the generated MIB file and trapd file. The system saves the generated artifacts in the same folder as that of the CADF file. Ensure that you have required disk space and file permissions.

### Procedure

1. At the prompt, type `cd $SPIRIT_HOME/scripts/utils.`
2. Type the following command:

```
generateTrapdAndMibUnix.sh [-l absolute path to cadf file] [-m MIB name] [-i MIB item name] [-p product ID] [-n product name] [-a author]
```

#### \* Note:

- If the path to the CADF file is incorrect, the system displays JVM errors.
- If the input to the **generateTrapdAndMibUnix.sh** command is invalid, the system displays No data or wrong data in .my and .conf files.

### Example

```
generateTrapdAndMibUnix.sh [-l /op/Avaya/SMGR_CommonAlarmDefn_Data.xml] [-m AV-AURA-SYSTEM-MANAGER-MIB] [-i avAuraSysMgr] [-p 25] [-n Avaya Aura System Manager] [-a Avaya]
```

### Related links

[generateTrapdAndMibUnix](#) on page 956

[Configuration files in the MIBTOOL.jar file](#) on page 955

## Configuration files in the MIBTOOL.jar file

The MIBTOOL.jar file contains the following property files in the `spirit/mibtool/staticfiles` location:

| File name      | Description                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------|
| MIB.properties | The file contains default values for MIB name, MIB item name, and product ID. You can change the values. |

*Table continues...*

| File name             | Description                                                                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MIBXMLTAGS.properties | The file contains tags in CADF file that contains the information for items such as alarm name and OID. If you change the CADF file format, you must configure the tag names accordingly in the property file. Separate the values by a comma. |

**\* Note:**

Do not edit the property files. If you must edit, use a program such as WinZip and open the MIBTOOL.jar file. Do not extract the files. To view the files, navigate to the `com/avaya/resource` directory. Open the file by with a text editor, make the changes, and save the file. When WinZip prompts, click **Choose update the zip archive with the changes**.

## generateTrapdAndMibUnix

The **generateTrapdAndMibUnix** converts the Common Alarm Definition File (CADF) xml file to MIB file (.my) and trapd (.conf) file. The tool converts only CADF files with notification OIDs that are specified in the X.X.X.productID.0.n format, where n is the notification OID.

### Syntax

```
generateTrapdAndMibUnix.sh [-l absolute path to cadf file] [-m MIB name] [-i MIB item name] [-p product ID] [-n product name] [-a author]
```

### Example

```
generateTrapdAndMibUnix.sh [-l /op/Avaya/SMGR/CommonAlarmDefn_Data.xml] [-m AV-AURA-SYSTEM-MANAGER-MIB] [-i avAuraSysMgr] [-p 25] [-n Avaya Aura System Manager] [-a Avaya]
```

### Considerations

You must provide all parameters. To provide the parameters later, you must edit the generated MIB file and trapd file. The system saves the generated artifacts in the same folder as that of the CADF file. Ensure that you have required disk space and file permissions.

## Managing SNMPv3 user profiles

### Creating an SNMPv3 user profile

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMPv3 User Profiles**.
3. Click **New**.
4. On the New User Profile page, complete the User Details section.
5. Click **Commit**.

### Related links

[SNMPv3 user profiles field descriptions](#) on page 958

## Editing an SNMPv3 user profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMPv3 User Profiles**.
3. Select the user profile you want to edit from the profile list.
4. Click **Edit**.
5. Edit the required fields in the Edit User Profile page.

 **Note:**

You cannot edit an SNMPv3 user profile that is assigned to the serviceability agent of an element or that is attached to a target profile.

6. Click **Commit**.

### Related links

[SNMPv3 user profiles field descriptions](#) on page 958

## Viewing an SNMPv3 user profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMPv3 User Profiles**.
3. Click the user profile you want to view from the profile list.
4. Click **View**.

You can view the details, except the password, of the SNMPv3 user profile in the View User Profile page.

### Related links

[SNMPv3 user profiles field descriptions](#) on page 958

## Deleting an SNMPv3 user profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMPv3 User Profiles**.
3. Select the user profile or profiles you want to delete from the profile list.
4. Click **Delete**.
5. On the User Profile Delete Confirmation page, click **Delete**.

 **Note:**

You cannot delete a user profile that is attached to an element or a target profile.

## Filtering SNMPv3 user profiles

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMPv3 User Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the User Profile List.
5. Click **Apply**.

To hide the column filters, click **Disable**. This action does not clear the filter criteria that you set in the column filters.

## SNMPv3 user profiles field descriptions

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Name</b>                       | <p>The SNMPv3 user name.</p> <p> <b>Note:</b></p> <p>The user name can contain the following characters: alphanumeric, period, underscore, white space, single quote, and hyphen. The user name cannot be blank.</p>                                                                      |
| <b>Authentication Protocol</b>         | <p>The authentication protocol used to authenticate the source of traffic from SNMP V3 users.</p> <p>The possible values are:</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> </ul> <p>The default is MD5.</p>                                                                                                                                        |
| <b>Authentication Password</b>         | <p>The password used to authenticate the user.</p> <p> <b>Note:</b></p> <p>The password can contain any printable and non-whitespace characters. The password must be at least 8 characters in length and can contain up to 255 characters. The password cannot be an empty string.</p> |
| <b>Confirm Authentication Password</b> | <p>The authentication password that you re-enter for confirmation.</p>                                                                                                                                                                                                                                                                                                     |

*Table continues...*



| Name                            | Description                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Privacy Protocol</b>         | The encryption policy for an SNMP V3 user.<br>The possible values are: <ul style="list-style-type: none"> <li>• DES: Use DES encryption for SNMP-based communication.</li> <li>• AES: Use AES encryption for SNMP-based communication.</li> <li>• None</li> </ul> The default value is AES. |
| <b>Privacy Password</b>         | The pass phrase used to encrypt the SNMP data.                                                                                                                                                                                                                                              |
| <b>Confirm Privacy Password</b> | Retype the privacy password in this field for confirmation.                                                                                                                                                                                                                                 |
| <b>Privileges</b>               | The privileges that determines the operations that you can perform on MIBs. <ul style="list-style-type: none"> <li>• Read/Write: Use to perform GET and SET operations.</li> <li>• Read: Use to perform only GET operation.</li> <li>• None.</li> </ul> The default is None.                |

| Button        | Description                                                                            |
|---------------|----------------------------------------------------------------------------------------|
| <b>Commit</b> | Use to create a new SNMPv3 user profile.<br>Saves the changes after an edit operation. |
| <b>Back</b>   | Cancels the action and returns to the previous page.                                   |
| <b>Delete</b> | Use to delete the user profiles you select.                                            |
| <b>Edit</b>   | Use to edit the user profile you select.                                               |

## Managing SNMP target profiles

### SNMP Target profile list

| Name                | Description                                                               |
|---------------------|---------------------------------------------------------------------------|
| <b>Name</b>         | The name of the SNMP target profile. This name should be a unique value.  |
| <b>Domain Type</b>  | The type of transport for the flow of messages. The default value is UDP. |
| <b>IP Address</b>   | The IP address of the SNMP target profile.                                |
| <b>Port</b>         | The port of the SNMP target profile.                                      |
| <b>SNMP Version</b> | The version of the SNMP protocol.                                         |

| Button                | Description                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------|
| <b>New</b>            | To go to the New Target Details page where you can add a new SNMP target profile.         |
| <b>View</b>           | To go to the View Target Details page where you can view an existing SNMP target profile. |
| <b>Edit</b>           | To go to the Edit Target Details page where you can edit an existing SNMP target profile. |
| <b>Delete</b>         | To delete the existing SNMP target profiles that you select.                              |
| <b>Filter: Enable</b> | To filter the SNMP target profiles list by one or multiple criteria.                      |

## Filtering target profiles

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMP Target Profiles**.
3. Click **Filter: Enable** above the Profile List.
4. Apply the filter to one or multiple columns of the Target Profile List.
5. Click **Apply**.

To hide the column filters, click **Disable**. This action does not clear the filter criteria that you set in the column filters.

## Creating an SNMP target profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMP Target Profiles**.
3. On the SNMP Target Profiles page, click **New**.
4. On the New Target Profiles page, complete the Target Details section.
5. **(Optional)** Click the **Attach/Detach User Profile** tab to attach a user profile.

Perform the step only if you select the SNMPv3 protocol.

6. Click **Commit**.

### Related links

[SNMP target profiles field descriptions](#) on page 962

## Viewing an SNMP target profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMP Target Profiles**.
3. From the Target Profile list, click the profile you must view.

4. Click **View**.

The system displays the details of the target profile in the View Target Details page.

#### Related links

[SNMP target profiles field descriptions](#) on page 962

## Editing an SNMP target profile

### About this task

#### **Note:**

Modify the target profiles that point to System Manager to reflect the changed IP address in the event of an IP address change on System Manager.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMP Target Profiles**.
3. In the Target Profile list, click the profile that you must edit.
4. Click **Edit**.
5. On the Edit Target Profiles page, modify the required fields.

#### **Note:**

You cannot edit a target profile that is assigned to the serviceability agent of an element. You must unassign the target profile before you edit the profile.

6. Click **Commit**.

#### Related links

[SNMP target profiles field descriptions](#) on page 962

## Deleting an SNMP target profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > SNMP Target Profiles**.
3. From the Target Profile list, click the profile or profiles you want to delete.
4. Click **Delete**.
5. On the Delete Confirmation page, click **Delete**.

#### **Note:**

You cannot delete a target profile that is attached to an element or an agent.

## SNMP target profiles field descriptions

| Name                     | Description                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>              | The name of the SNMP target profile.                                                                                  |
| <b>Description</b>       | The description of the SNMP target profile.                                                                           |
| <b>IP Address</b>        | The IP address of the target.                                                                                         |
| <b>Port</b>              | The port number of the target.                                                                                        |
| <b>Domain Type</b>       | The type of the message flow. The default is UDP.                                                                     |
| <b>Notification Type</b> | The type of notification. The options are: <ul style="list-style-type: none"> <li>• Trap</li> <li>• Inform</li> </ul> |
| <b>Protocol</b>          | The type of the SNMP protocol.                                                                                        |

| Button        | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Creates the target profile in the New Target Profile page or saves the changes in the Edit Target Profile page. |
| <b>Back</b>   | Cancels your action and returns to the previous page.                                                           |

## Notification filtering

### Notification filtering

System Manager supports alarm filtering capability. With filtering, you can select a product that System Manager supports to send filtered alarms only to specific targets.

When you send notifications to System Manager, SAL Gateway or other Network Management System (NMS), you can exclude or include notifications from elements. You can create filter profiles and assign the profiles to the target and serviceability agent pair. You can also remove the profiles from the target and serviceability agent pair. You can select alarms that you want to receive from a product on NMS. NMS can be System Manager or a third-party NMS system.

For a product, you can define the filter criteria to receive notifications on the target serviceability agent from the specific OIDs or block notifications on the target serviceability agent from the specific OIDs.

For example:

- To receive only major alarms from Session Manager, you must create a filter profile for Session Manager, select all major alarm OIDs and assign the filter profile to the target NMS for the serviceability agent of that Session Manager so that the target receives only the alarms specified in the filter profile.
- To block warning or minor alarms from Session Manager, you must create a filter profile for the product Session Manager, select exclude option and select OIDs of type warning and minor, and then assign the filter profile to the target NMS for the serviceability agent of

Session Manager so that the target does not receive warnings and minor alarm notifications from that Session Manager.

## Creating a notification filter profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Notification Filter Profile**.
3. On the Filter Profiles page, click **New**.
4. On the New Filter Profile page, click the **Filter Profile Details** tab and complete the fields.
5. Click **Exclude** or **Include**.

The default is Include.

For more information, see Create, View, Edit, or Delete Filter Profiles field descriptions.

6. Click the **Attach/Detach Notification Oids** tab, perform the following:
  - a. In the **Notification Subtree** field, type a value that ends with dot star (.\* ) and click **Add**.  
For example, 6889.2.35.\*  
System Manager excludes or includes alarms from the notification IDs that you select.

#### **Note:**

- If you perform Step 6a, Step 6b and Step 6c are optional.
  - If you perform Step 6b and Step 6c, Step 6a is optional.
- b. In the **Select Notifications** section, in the **Products** field, select a product.
  - c. In the notification list, select one or more notification IDs.
7. Click **Commit**.

### Related links

[Create, View, Edit, or Delete Filter Profiles field descriptions](#) on page 966

[Filter Profiles field descriptions](#) on page 966

[Assigning filter profile to a serviceability agent](#) on page 964

[Unassigning the filter profile from a serviceability agent](#) on page 965

## Viewing the notification filter profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Notification Filter Profile**.
3. On the Filter Profiles page, select a filter profile and click **View**.

4. On the View Filter Profile page, review the fields on the following tabs:
  - **Filter Profile Details**
  - **Attach/Detach Notification Oids**
5. Click **Done**.

#### Related links

[Create, View, Edit, or Delete Filter Profiles field descriptions](#) on page 966  
[Filter Profiles field descriptions](#) on page 966

## Editing notification filter profiles

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Notification Filter Profile**.
3. On the Filter Profiles page, select a filter profile and click **Edit**.
4. On the Edit Filter Profile page, complete the following:
  - a. Click the **Filter Profile Details** tab and complete the fields.  
For more information, see [Create, View, Edit, or Delete Filter Profiles field descriptions](#).
  - b. Click the **Attach/Detach Notification Oids** tab and complete the fields.
5. Click **Commit**.

#### Related links

[Create, View, Edit, or Delete Filter Profiles field descriptions](#) on page 966  
[Filter Profiles field descriptions](#) on page 966

## Deleting the notification filter profile

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Notification Filter Profile**.
3. On the Filter Profiles page, select a filter profile and click **Delete**.
4. On the Filter Profile Delete Confirmation page, click **Delete**.

#### Related links

[Create, View, Edit, or Delete Filter Profiles field descriptions](#) on page 966  
[Filter Profiles field descriptions](#) on page 966

## Assigning filter profile to a serviceability agent

### Procedure

1. On the System Manager web console, click **Services > Inventory**.

2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. Select a product for which you created the filter profile.
4. Click **Manage Profiles**.

The system displays the serviceability agent in the **Selected Agents** section.

5. Click the **SNMP Target Profiles** tab, select System Manager or the third-party NMS target agent, and click **Assign**.

The system displays the target in the list.

6. To assign the filter profile from the serviceability agent, perform the following:

- a. In the **Removable Profiles** section, select the target.

The **Assign/Remove Filter Profile** link becomes active.

- b. Click **Assign/Remove Filter Profile**.

7. In the **Profile List** section, click the plus sign (+).

The system displays the filter profile that you selected in the **Assigned Filter Profiles** section.

 **Note:**

You can assign only one filter profile to the target agent for a serviceability agent. For example, for a Session Manager serviceability agent, if the target is System Manager, then you can add only one filter profile to the System Manager target for the same Session Manager system.

8. Click **Commit**.

The system assigns the filter profile to the serviceability agent.

#### Related links

[Unassigning the filter profile from a serviceability agent](#) on page 965

## Unassigning the filter profile from a serviceability agent

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. Select a product for which you created the filter profile.
4. Click **Manage Profiles**.

The system displays the serviceability agent in the **Selected Agents** section.

5. Click the **SNMP Target Profiles** tab.

6. In the **Removable Profiles** section, select the target.

The **Assign/Remove Filter Profile** link becomes active.

7. Click **Assign/Remove Filter Profile**.

8. In the **Assigned Filter Profiles** section, click the minus sign (-).

The system displays the filter profile in the **Profile List** section.

9. Click **Commit**.

The system disassociates the filter profile from the serviceability agent.

#### Related links

[Assigning filter profile to a serviceability agent](#) on page 964

### Filter Profiles field descriptions

| Name               | Description                                  |
|--------------------|----------------------------------------------|
| <b>Name</b>        | The name of the notification filter profile. |
| <b>Description</b> | A description of the notification profile.   |

| Button        | Description                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------|
| <b>New</b>    | Displays the New Filter Profile page where you can create a notification filter profile.                      |
| <b>View</b>   | Displays the View Filter Profile page where you can view a notification filter profile.                       |
| <b>Edit</b>   | Displays the Edit Filter Profile page where you can view a notification filter profile.                       |
| <b>Delete</b> | Marks the notification filter profile that you select. You must confirm for the system to delete the profile. |

### Create, View, Edit, or Delete Filter Profiles field descriptions

#### Filter Profile Details

| Name                                    | Description                                                                                                                                                                                      |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                             | The name of the notification filter profile.                                                                                                                                                     |
| <b>Description</b>                      | A description of the notification filter profile.                                                                                                                                                |
| <b>Specify Include/Exclude criteria</b> | <p>An option to include or exclude the notification OIDs.</p> <ul style="list-style-type: none"> <li>• <b>Include</b></li> <li>• <b>Exclude</b></li> </ul> <p>The default is <b>Include</b>.</p> |



## Attach/Detach Notification Oids Specify Notification Subtrees

| Name                        | Description                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Notification Subtree</b> | The notification subtree that you want to add to the subtree list.<br><br>The value you enter must end with dot followed by asterisk (.*), for example, 6889.4.*. Otherwise the system does not add notification subtree to the list. |
| <b>Add</b>                  | Adds the notification subtree to the list.                                                                                                                                                                                            |

## Specify Notifications

| Name           | Description                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Product</b> | The product for which you want to filter the notifications while sending notifications to System Manager, SAL Gateway or other NMS systems. |

| Button        | Description                                                                |
|---------------|----------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes made to the page and returns to the Filter Profile page. |
| <b>Back</b>   | Discards the changes and returns to the Filter Profile page.               |

## Managing user and target profiles

### Automatic activation of serviceability agents

For newly installed elements that work with Release 6.3.8 serviceability agents, you do not need to manually activate the agents from the Manage Serviceability Agent page. System Manager automatically activates the agents. In the **Agents List** section, the system displays the agent as Active. You can assign the target or user profiles to the agent that is automatically activated.

#### **Note:**

The auto activate functionality only applies to serviceability agents added in Release 6.3.5 or later. If you recover an agent by running the **recoverAgent** script, then the system adds the agent after receiving the next heartbeat message. The system automatically activates the recovered agent.

### Repairing serviceability agents

#### About this task

If the alarming functionality of an element fails, you can repair the serviceability agent. The repair process triggers the SNMP configuration.

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.

2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. In the **Agent List** section, select one or more active agents that you want to repair.
4. Click **Repair Serviceability Agent**.

The system starts the SNMP configuration of the serviceability agent. At the subsequent heartbeat of the agent, the system notifies System Manager about the start of the SNMP configuration. Therefore, wait for about 15 minutes, the heartbeat interval, to test alarms from the element.

When System Manager receives the subsequent heartbeat, the system reactivates the agent. The system also assigns the target profiles and user profiles to the agent and the alarming functionality starts working.

5. **(Optional)** To make the changes immediately, log in to the server on which the serviceability agent runs and type `service spiritAgent restart`.

You can perform this step if you do not want to wait for the next heartbeat of the agent.

## Activating a serviceability agent

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. In the **Agent List** section, select one or more agents that you must activate.
4. Click **Activate**.

The system activates the SNMPv3 functionality in the remote serviceability agent that you selected. If the system does not activate the SNMPv3 functionality, refresh the Web page and repeat Step 3 and Step 4.

### Related links

[Managing SNMPv3 user profiles for the selected serviceability agents](#) on page 969

[Managing target profiles for the selected serviceability agents](#) on page 968

## Managing target profiles for the selected serviceability agents

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. In Agent List, select the active agents that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMP Target Profiles** tab.
6. Select the target profiles you must assign from the Assignable Profiles section.
7. Click **Assign**.

You can unassign or remove target profiles from the Removable Profiles section by clicking **Remove**.

8. Click **Commit** to assign the profiles to the selected agent.

 **Note:**

You can also select more than one serviceability agents and assign the same target profiles to all the agents.

#### Related links

[Activating a serviceability agent](#) on page 968

[Managing SNMPv3 user profiles for the selected serviceability agents](#) on page 969

## Managing SNMPv3 user profiles for the selected serviceability agents

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. In the **Agent List** section, select an active agent that you must manage.
4. Click **Manage Profiles**.
5. Click the **SNMPv3 User Profile** tab.
6. In the **Assignable Profiles** section, select the user profiles that you want to assign.
7. Click **Assign**.

To remove user profiles, in the **Removable Profiles** section, select the user profiles and click **Remove**.

8. To assign the user profiles to the selected agent, click **Commit**.

 **Note:**

You can also select more than one serviceability agents and assign the same user profiles to all agents.

#### Related links

[Activating a serviceability agent](#) on page 968

[Managing target profiles for the selected serviceability agents](#) on page 968

## Managing the status of manage profile job for an agent

### About this task

From Release 8.1, when you perform manage profile for more than one agent, the system creates a background job.

Use this procedure to view and retry the manage profile job for agents.

Manage Profile for single agent is the same. The system does not create a job for single agent.

## Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. On the Serviceability Agents page, click **Manage Profile Job Status**.

System Manager displays the Manage Profile Jobs page with **Job Name**, **Status**, **Total Agents**, **Failed Agents**, **Job Start Time**, and **Job End Time**.

4. To view the details, in the Manage Profile Jobs section, select a job name, and click **View Details**.

System Manager displays the Failed Agents Detail For Job - <Job\_Name> section with **Agent IP Address**, and **Error Details**.

When you hover on **Job Name**, the system displays a brief description about the job, which target is added or removed, and which user is added or removed.

5. To retry the operation for the failed agent, perform the following:
  - a. Select one or more agent IP Address.
  - b. Click **Retry Operation**.

System Manager displays the Serviceability Agents page with the list of the failed agents that you selected for retrying any operation.

You can use the **Reset Table** button on the Serviceability Agents page to display all the agents.

- c. Click **Close** to close the Failed Agents Detail For Job - <Job\_Name> section.
6. Click **Back** to return to the Serviceability Agents page.

## Serviceability Agents field descriptions

### Agent List

| Name               | Description                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hostname</b>    | The host name of the server on which the serviceability agent runs.                                                                        |
| <b>IP Address</b>  | The IP address of the server on which the serviceability agent runs.                                                                       |
| <b>System Name</b> | The system name of the server on which the serviceability agent runs.                                                                      |
| <b>System OID</b>  | The system OID of the server on which the serviceability agent runs.                                                                       |
| <b>Status</b>      | The enabled or disabled status of the serviceability agent. The system disables SNMPv3 and displays <b>Inactive</b> as the default status. |

| Button                 | Description                                                         |
|------------------------|---------------------------------------------------------------------|
| <b>Activate</b>        | Activates one or more Serviceability Agent.                         |
| <b>Manage Profiles</b> | Manages the target profiles for the selected serviceability agents. |

*Table continues...*

| Button                             | Description                                                                                                                                                                                                                                                                                                            |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generate Test Alarm</b>         | Generates test alarms from the System Manager web console for agents, hosts, or elements that are installed with Serviceability Agents                                                                                                                                                                                 |
| <b>Repair Serviceability Agent</b> | Repairs the serviceability agent.                                                                                                                                                                                                                                                                                      |
| <b>Manage Profile Job Status</b>   | Manages the profile job for the serviceability agent.                                                                                                                                                                                                                                                                  |
| <b>Reset Table</b>                 | When you perform the retry operation on the Manage Profile Job Status page, System Manager displays the list of failed agents on the Serviceability Agents page. If you need to clear the list of failed agent list and display all the available agents in the Agent List section, use the <b>Reset Table</b> button. |
| <b>Advanced Search</b>             | The link to perform advance search. When you click on this link, System Manager displays the Criteria section.                                                                                                                                                                                                         |
| <b>Filter: Enable</b>              | The fields where you can set the filter criteria. <b>Filter: Enable</b> is a toggle button.                                                                                                                                                                                                                            |
| <b>Filter: Disable</b>             | Hides the column filter fields. <b>Filter: Disable</b> is a toggle button.                                                                                                                                                                                                                                             |
| <b>Filter: Apply</b>               | Filters agents based on the filter criteria.                                                                                                                                                                                                                                                                           |
| <b>Select: All</b>                 | Selects all agents in the table.                                                                                                                                                                                                                                                                                       |
| <b>Select: None</b>                | Clears the selection for the agents that you select.                                                                                                                                                                                                                                                                   |
| <b>Refresh</b>                     | Refreshes the agent information in the table.                                                                                                                                                                                                                                                                          |

## Criteria

| Name                          | Description                                                                                                                                                                                                                                                                |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Search Criteria</b> | The options are: <ul style="list-style-type: none"> <li>• <b>Hostname</b></li> <li>• <b>IP Address</b></li> <li>• <b>System Name</b></li> <li>• <b>Device Type</b></li> <li>• <b>System OID</b></li> <li>• <b>Target Profile</b></li> <li>• <b>User Profile</b></li> </ul> |
| <b>Select Search Operator</b> | The options are: <ul style="list-style-type: none"> <li>• <b>Equals</b></li> <li>• <b>Not Equals</b></li> <li>• <b>Starts with</b></li> <li>• <b>Ends with</b></li> <li>• <b>Contains</b></li> </ul>                                                                       |
| <b>Enter Search to Text</b>   | Specify the search criteria.                                                                                                                                                                                                                                               |

| Button | Description                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------|
| -      | Removes the additional search criteria fields.<br>This field is enabled when the additional search criteria fields are added. |
| +      | Adds the additional search criteria fields.                                                                                   |
| Clear  | Clears the search criteria.                                                                                                   |
| Search | Performs the search for the specified search criteria                                                                         |
| Close  | Closes the Criteria section.                                                                                                  |

---

## Synchronization of Data

---

### Communication Manager, Messaging data, and IP Office synchronization

Elements that System Manager manages have alternative ways of administering data. To ensure uniformity in the database when a variety of tools are used, you can use the synchronization menu. You can synchronize Communication Manager, Messaging, and IP Office data through this menu.

#### Communication System

Using System Manager, you can synchronize the System Manager data with Communication Manager. When you add Communication Manager to the system, System Manager automatically initiates synchronization to update the System Manager database.

#### Initializing synchronization

With initializing synchronization, you can synchronize the data in the System Manager database with each managed Communication Manager system. When you add a Communication Manager into the system, System Manager automatically initiates an initialization task to get the required Communication Manager data, and stores the data in the System Manager database.

#### Important:

If there is a change in any of the following Communication Manager objects in Communication Manager, you must initiate full initialization synchronization of this Communication Manager in System Manager.

- system-param features
- system-param cdr
- system-param cust
- system-param spec
- system-param security

- system-param country-options
- system-param maintenance
- dialplan
- cabinet
- board

### Incremental synchronization

With incremental synchronization with selected devices, you can incrementally synchronize the data in the System Manager database with each managed Communication Manager system. This synchronization updates the changed data in the database in Communication Manager since synchronization was last run.

Once the first Initialization synchronization job gets completed, System Manager schedules recurring Incremental synchronization job at every 24 hour.

Incremental synchronization pulls all the incremental commands from the Communication Manager command history, which are performed on Communication Manager after last Communication Manager synchronization and that are executed on Communication Manager by the Communication Manager user that is not available in the System Manager inventory.

Incremental synchronization does not pull the station, if the station is added on Communication Manager by the same Communication Manager user that is in available in the System Manager inventory.

#### Important:

Though you perform an incremental synchronization, System Manager initiates an initializing synchronization when you:

- Upgrade System Manager. The system displays the synchronization status as **SMGR Upgraded**, and you can continue to perform the administrative tasks even after System Manager is upgraded.
- Upgrade or rollback Communication Manager.

System Manager initiates initializing synchronization instead of incremental synchronization in the following scenarios:

- At the time of every incremental synchronization, System Manager verifies the Communication Manager version and if the version is greater than the existing Communication Manager version (for example, Communication Manager is upgraded), then System Manager starts the initialization synchronization.
- Last initializing synchronization status is failed.
- If count of command history is more than 1800.

#### Note:

If the CM notify sync feature is enabled on the system, then incremental synchronization does not synchronize Communication Manager commands processed by the CM notify sync feature.

## IP Office system

With System Manager, you can synchronize the System Manager data with IP Office. When you add a new IP Office device to System Manager, System Manager automatically initiates synchronization to update the System Manager database.

## Messaging data

You can also synchronize the messaging data in System Manager with Messaging, Communication Manager Messaging, and Modular Messaging systems.

### **Note:**

Before you perform synchronization, you must add a new Communication Manager or a messaging entity from Manage Elements.

## Scheduled synchronization

You can create and schedule synchronization jobs using System Manager. You can schedule a synchronization job to run at a fixed time and repeat it periodically. System Manager provides a default incremental synchronization every 24 hours. You can modify this to your convenience.

## On-demand synchronization

With System Manager, you can synchronize data with Communication Manager on demand. Administrators can initiate this synchronization at any time. On-demand synchronization can be an initialization synchronization or an incremental synchronization.

### Related links

[Initializing synchronization](#) on page 975

[Initializing incremental synchronization](#) on page 975

[Saving the Communication Manager translations](#) on page 978

---

# Synchronizing the Communication Manager data and configuring options

## Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Synchronization > Communication System**.
3. Select the Communication Manager device that you want to synchronize.
4. Select one of the following options that you want to synchronize for the selected device:
  - **Initialize data for selected devices:** To synchronize data in the System Manager database with each managed Communication Manager system.

### **Note:**

When you add a Communication Manager instance to the system, System Manager automatically initiates an initialization task to get all the required Communication Manager data and stores the data in the System Manager database.



- **Incremental Sync data for selected devices:** To synchronize incrementally the selected devices data in the System Manager database with each managed Communication Manager system.

 **Note:**

This synchronization updates the data in the database in Communication Manager that is changed since last synchronization.

- **Execute 'save trans all' for selected devices:** To save the configuration of the selected device on the same device, Communication Manager itself.

5. Perform one of the following:

- To perform the synchronization now, click **Now**.
- To perform the synchronization at a specified time, click **Schedule**.

 **Note:**

To view the status of synchronization, on the System Manager web console, click **Services > Scheduler**.

---

## Initializing synchronization

### Procedure

1. On the System Manager web console, click **Services > Inventory > Synchronization > Communication System**.
2. On the Synchronize CM Data and Configure Options page, select the Communication Manager entities.
3. Select **Initialize data for selected devices**.
4. Do one of the following:
  - To perform the synchronization immediately, click **Now**.
  - To perform the synchronization at a specified time, click **Schedule**.

---

## Initializing incremental synchronization

### Procedure

1. On the System Manager web console, click **Services > Inventory > Synchronization > Communication System**.
2. On the Synchronize CM Data and Configure Options page, select the Communication Manager system that you want to synchronize.
3. Select **Incremental Sync data for selected devices**.

4. Do one of the following:

- To perform the incremental synchronization immediately, click **Now**.
- To perform the incremental synchronization at a specified time, click **Schedule**.

 **Note:**

While scheduling incremental synchronization, set the logging levels on Communication Manager using the **change logging-levels** option. In the **Log Data Values** field, select `both`.

When you add a Communication Manager system, the default incremental synchronization jobs will be scheduled 1 hour after the maintenance job starts on Communication Manager.

If the incremental synchronization of the Communication Manager data fails due to the overlapping of Communication Manager synchronization and maintenance jobs, change the default scheduled job time in the Pending Jobs page.

---

## Synchronizing the IP Office system configuration

### Procedure

1. On the System Manager console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **IP Office**.
3. Select the device you want to synchronize.
4. Below the device list, select any of the following options that you want to synchronize for the selected device:
  - **System Configuration:** This option enables you to get the latest system configuration of the device and update the same in System Manager.
  - **User:** This option enables you to synchronize all the users present in System Manager from the selected device.
  - **System Configuration and Users:** This option enables you to get the latest system configuration and details of all the users from the selected device and synchronize with System Manager.
5. Click **Now** to perform the synchronization now or click **Schedule** to perform the synchronization at a specified time.

 **Note:**

To view the status of synchronization, click **Services** > **Scheduler** on the System Manager console.

## Synchronizing the UCM and Application Server system configuration

### About this task

Use the procedure to synchronize the configuration of a UCM and Application Server device with the local machine.

### Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **UCM and Application Server**.
3. Select the device that you want to synchronize.

**System Configuration** is selected by default.

4. Do one of the following:
  - To perform the synchronization now, click **Now**.
  - To perform the synchronization at a specified time, click **Schedule**.
5. To view the status of synchronization, click **Services** > **Scheduler**.

## Synchronizing the VMPro system configuration

### Before you begin

To synchronize VMPro devices successfully, perform the following:

- Configure VMPro IP Address in IP Office System Configuration.
- Password of VMPro should be same for IP Office, UCM and Application Server and VMPro System Preferences.

#### **Note:**

- You can change the password for Application Server through security setting using IP Office Manager.
- You can change the password for VMPro System Preferences through Web Manager.
- You must give access rights to VMPro Application from security setting of IP Office and UCM and Application Server through IP Office Manager.
- You must have valid IP Office licenses for VMPro instances.

### Procedure

1. On the System Manager console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **VMPro**.
3. Select the device you want to synchronize.

4. In the device list, select any of the following options that you want to synchronize for the selected device.
5. Click **Now** to perform the synchronization now or click **Schedule** to perform the synchronization at a specified time.

 **Note:**

To view the status of synchronization, click **Services** > **Scheduler** on the System Manager console.

## Result

If the operation of synchronizing the VMPro succeeds, you can work on the latest updated vmpro system configuration and avoid data corruption.

If the operation of synchronizing the VMPro fails, you can work only on local available system configuration in System Manager.

If the operation of synchronizing the VMPro fails and if it is first time that you attempted data synchronization, you can work only on the default configuration.

---

## Synchronizing the messaging data

### Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Synchronization** > **Messaging System**.
3. Select the messaging systems that you want to synchronize.
4. Perform one of the following:
  - Click **Now** to perform the synchronization now.
  - Click **Schedule** to perform the synchronization at a specified time.

---

## Saving the Communication Manager translations

### Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the navigation pane, click **Synchronization** > **Communication System**.
3. From the list select a Communication Manager system.
4. Select **Execute 'save trans all' for selected devices**.
5. To save the System Manager administration changes in Communication Manager, click **Now**.

To save the translations at a specified time, click **Schedule**.

 **Note:**

After running the **Save translation job**, the system may not update the last saved translation time in the Communication Manager list. This might be because the save translation operation is slow when Communication Manager has large data or translations to save. In such conditions, the system updates the last saved translation time only on the next incremental synchronization after the save translations operation is complete on Communication Manager.

---

## About CM audit

You can perform a CM audit for those Communication Managers that are synchronized with System Manager. You can select one or more Communication Managers and perform the audit. After the audit is completed, you can view the results by clicking **View Audit Report**. This audit report comprises the audit summary or a snapshot of the changes, and the audit details or the detailed report of the changes.

---

## Performing a Communication Manager audit

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Synchronization > Communication System**.
3. Select the Communication Managers that you want to audit.
4. Click **Audit**.
5. Click **Now**.  
To schedule the audit at a later time, click **Schedule**.
6. To view the audit report, click **View Audit Report**.
7. On the Audit Info page, select the job name, and click **View**.

### Related links

[Audit report field descriptions](#) on page 980

[CM audit field descriptions](#) on page 979

---

## CM audit field descriptions

| Name     | Description                |
|----------|----------------------------|
| Job Name | The name of the audit job. |

*Table continues...*

| Name              | Description                                                                             |
|-------------------|-----------------------------------------------------------------------------------------|
| <b>Job Status</b> | The status of the job. Specifies whether the audit job is pending, failed, or complete. |
| <b>Start Time</b> | The start time of the audit job.                                                        |
| <b>End Time</b>   | The end time of the audit job.                                                          |

| Button      | Description                                                       |
|-------------|-------------------------------------------------------------------|
| <b>View</b> | Click to go to the audit report page.                             |
| <b>Done</b> | Click to complete the current action and go to the previous page. |

---

## Audit report field descriptions

| Name                  | Description                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------|
| <b>Object Name</b>    | The name of the Communication Manager object that is audited.                                            |
| <b>Identifier</b>     | The identifier for the Communication Manager object.                                                     |
| <b>CM</b>             | The <b>CM</b> field specifies all the changes in Communication Manager after the audit is complete.      |
| <b>System Manager</b> | The <b>System Manager</b> field specifies all the changes in System Manager after the audit is complete. |

| Button      | Description                       |
|-------------|-----------------------------------|
| <b>Done</b> | Click to go to the previous page. |

---

## Communication Profiles synchronization

---

### Communication profiles synchronization

System Manager provides the account synchronization feature to synchronize profiles between CS 1000 communication profile and their elements. Using this feature you can synchronize profiles in User Management with the profiles in the elements. During synchronization, the account synchronization feature uses the account data in the elements as the master data. Therefore, when a profile data is not in synchronization with the element, the account data from the element is copied to System Manager.

 **Note:**

- The account synchronization feature updates the UPM CS 1000 communication profile with data from the CS 1000 element, and deletes the communication profiles that are linked to phones or mailboxes that do not exist in the CS 1000 element.

- If the data, such as, DN, mailbox, and TN has been modified on the CS 1000 element, the system provisions the data to System Manager UPM during account synchronization feature, but the CPND name and **Mailbox Number** are provisioned from System Manager UPM to the CS 1000 element.
- The system maps the CPND name of the CS 1000 element to the System Manager UPM user **Localized Display Name**.

Common scenarios are:

- If the System Manager UPM user first and last names are the same as the phone CPND name (For example: first = "John", last = "Smith", CPND = "John Smith" or CPND = "John, Smith" if display format = "first, last") on the CS 1000 element, then the system links the phone with this user and creates communication profile during the account synchronization process.
- If **Localized Display Name** is changed in the System Manager UPM user and this user has communication profile linked to the CS 1000 phones, the system immediately provisions the CPND name to the CS 1000 phone without using the account synchronization process.
- If the CPND name is changed on the CS 1000 element, the changes will be lost during the account synchronization process, and the system overwrites the CPND name by **Localized Display Name** from the System Manager UPM user.

---

## Synchronizing the CS 1000 profile

### Before you begin

Register all CS 1000 element on System Manager 6.2 or later.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Synchronization > CS 1000 and CallPilot Synchronization**.
3. Select the element that you want to synchronize.
4. Click **Start** to start the synchronization process.

 **Note:**

For the average duration of operations of the CS 1000 element, see Average duration of CS 1000 account operations.

5. **(Optional)** Do one of the following:
  - Click **Stop** to stop the synchronization process.  
The system disables all other buttons when you click **Stop**.
  - Click **Clear** to clear the synchronization information that the system displays.
  - Click **Reload** to refresh.

## Related links

- [Bulk importing of users](#) on page 379
- [Exporting users in bulk from web console](#) on page 383
- [Synchronize communication profiles field descriptions](#) on page 983
- [Average duration of CS 1000 account operations](#) on page 985

---

## Assigning anonymous profiles

### About this task

When the synchronization process is complete, the **Summary** column displays any anonymous accounts in the element. You can assign the anonymous account to users or delete the account from the element.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Synchronization > CS 1000 and CallPilot Synchronization**.
3. On the Synchronize Communication Profiles page, in the **Summary** column, click the anonymous profile that you want to assign.

The system displays the Anonymous Communication Profiles page with the details of each anonymous account.

4. Select one of the anonymous accounts.
5. In the **Name (Last, First)** field, enter the name of the user to whom you want to assign this communication profile.
6. Click **Assign**.

The system refreshes the Anonymous Communication Profiles page and displays the status of the assigned account.

## Related links

- [Anonymous Communication Profiles field descriptions](#) on page 984

---

## Deleting anonymous profiles

### About this task

You can delete the anonymous account from the element.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Synchronization > CS 1000 and CallPilot Synchronization**.



3. On the Synchronize Communication Profiles page, click the anonymous profile you want to delete from the **Summary** column.

The system displays the Anonymous Communication Profiles page with the details of each anonymous account.

4. Select the anonymous account you want to delete.
5. Click **Delete**.

The system displays a confirmation dialog box.

6. Click **OK**.

---

## Cleaning up communication profiles

### About this task

When you delete the CS 1000 element from the System Manager web console, the communication profiles linked to the element still exist in User Management. You can use the CS 1000 communication profile cleanup feature to permanently delete all accounts of elements that do not exist in the System Manager registry.

### Before you begin

The system does not delete the communication profiles of the soft deleted users. Therefore, before you run the cleanup, restore the soft deleted users.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Synchronization > CS 1000 and CallPilot Synchronization**.
3. Click **CleanUp**.
4. To confirm the operation, click **OK**.

---

## Synchronize communication profiles field descriptions

| Name    | Description                     |
|---------|---------------------------------|
| Element | The name of the CS 1000 system. |

*Table continues...*

| Name           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Status</b>  | <p>The current status of the synchronization process. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>Queued</b>: The synchronization task is queued and runs automatically when once other synchronization tasks are complete.</li> <li>• <b>Running</b>: The synchronization is running. The system displays the status when you click <b>Start</b>.</li> <li>• <b>Stopping</b>: The synchronization stops when you click <b>Stop</b>.</li> <li>• <b>Aborted</b>: The system displays this status when the synchronization stops completely.</li> <li>• <b>PASS</b>: Indicates that the synchronization is complete.</li> <li>• <b>FAIL</b>: Indicates that the synchronization has failed. You can view the log files to get the details of failure.</li> </ul> |
| <b>Date</b>    | The date when the synchronization started.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Summary</b> | <p>The number of accounts:</p> <ul style="list-style-type: none"> <li>• Processed</li> <li>• Anonymous accounts</li> <li>• Added, updated, and deleted</li> </ul> <p>When no accounts are processed, this field displays 0 account(s) processed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Button        | Description                                                   |
|---------------|---------------------------------------------------------------|
| <b>Start</b>  | Starts a synchronization process.                             |
| <b>Stop</b>   | Stops a synchronization process that is in the running state. |
| <b>Clear</b>  | Clears all the synchronization results that are processed.    |
| <b>Reload</b> | Refreshes the synchronization status once again.              |

## Anonymous Communication Profiles field descriptions

| Field                      | Description                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name (Last, First)</b>  | The name of the user to whom you must assign this communication profile.                                                                       |
| <b>Service Information</b> | The service information of the CS 1000 system.                                                                                                 |
| <b>Target</b>              | The customer number of the system for the element.                                                                                             |
| <b>Status</b>              | <p>The status of the anonymous profile. The options are:</p> <ul style="list-style-type: none"> <li>• Assigned</li> <li>• Anonymous</li> </ul> |

| Button        | Description                                                       |
|---------------|-------------------------------------------------------------------|
| <b>Assign</b> | Assigns the user to the anonymous profile that you select.        |
| <b>Delete</b> | Deletes the anonymous profile that you select after confirmation. |
| <b>Cancel</b> | Cancels the assign or delete action and opens the previous page.  |

#### Related links

[Average duration of CS 1000 account operations](#) on page 985

## Average duration of CS 1000 account operations

| Operation         | Duration in seconds |
|-------------------|---------------------|
| Account add       | 9                   |
| Account update    | 1                   |
| Account delete    | 1                   |
| Account anonymous | 0.1                 |

## Connection pooling

### Connection pooling

Connection pooling facilitates reuse of port connections. You can use System Manager to create a connection pool to reserve port connections to perform administrative and maintenance tasks on Communication Manager. Through the web interface, you can reserve 0 to 60 port connections across all Communication Manager elements, depending on the System Manager profile. If you exceed the number of port connections that can be pooled, the system displays an error message.

## Configuring Communication Manager Connection Pool

### About this task

Use this page to create or edit the connection pools in the System Manager.

System Manager uses OSSI and PCTT port connections. Connection pooling in System Manager pools only PCTT port connections. PCTT port connections manage the cut-through and provisioning through Classic View.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the left navigation pane, click **Connection Pooling**.

3. Click **Communication System**.

The system displays the Configure CM Connection Pool page.

4. In the **Connections Requested** field, type the number for each Communication Manager element in the table.

Depending on the System Manager profile, the number can be between 0 and 60 port connections across all Communication Manager elements.

 **Note:**

If you are configuring  $n$  connections in System Manager connection pooling, the **Maximum Number of Simultaneous logins for a user** field on the Communication Manager System Management interface must be  $n+1$ , so that Communication Manager allows you to acquire and pool all requested connections.

5. **(Optional)** To stop the connection pool, type 0 in the **Connections Requested** field.

6. Click **Commit**.

The system:

- Changes the **Status** field to Pooling Scheduled.
- Displays the number of connections assigned to the CM element in the **Connections Attained** field.
- Changes the **Status** field to Pooling Complete.

7. **(Optional)** To set a common pool size to all Communication Manager elements, perform the following:

- a. Select the **Set Common pool size for all the CMs** check box.
- b. In the **Set Common pool size for all the CMs** field, type the number for all Communication Manager elements in the table.
- c. **(Optional)** To stop the connection pool for all Communication Manager elements, type 0 in the **Set Common pool size for all the CMs** field.
- d. Click **Commit**.

The system:

- Changes the **Connections Requested** field to the number for all Communication Manager elements in the table.
- Changes the **Status** field to Pooling Scheduled.
- Displays the number of connections assigned to the Communication Manager element in the **Connections Attained** field.
- Changes the **Status** field to Pooling Complete.

## Connection Pooling field descriptions

| Name                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Set Common pool size for all the CMs</b> | <p>The field where the administrator sets a common number to reserve port connections for all Communication Manager elements.</p> <p> <b>Note:</b></p> <p>If you are configuring <math>n</math> connections in System Manager connection pooling, the <b>Maximum Number of Simultaneous logins for a user</b> field on the Communication Manager System Management interface must be <math>n+1</math>, so that Communication Manager allows you to acquire and pool all requested connections.</p> |
| <b>Element Name</b>                         | The name of the Communication Manager element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Connections Requested</b>                | <p>The number of port connections the administrator wants to reserves for the Communication Manager element.</p> <p> <b>Note:</b></p> <p>If you are configuring <math>n</math> connections in System Manager connection pooling, the <b>Maximum Number of Simultaneous logins for a user</b> field on the Communication Manager System Management interface must be <math>n+1</math>, so that Communication Manager allows you to acquire and pool all requested connections.</p>                  |
| <b>Status</b>                               | <p>The status of the connection pool for the Communication Manager element.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• NOT POOLED</li> <li>• POOLING SCHEDULED</li> <li>• POOLING COMPLETE</li> </ul>                                                                                                                                                                                                                                                                                                                                                     |
| <b>Connections Attained</b>                 | The number of port connections the system is able reserves for the Communication Manager element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Connections In Use</b>                   | The number of port connections the system is using from the pool of connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Idle Connections</b>                     | The number of port connections that are idle in the pool of connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Connections Used Outside Pool</b>        | The number of port connections that are outside the connection pool and are in use.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Button                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Commit</b>                               | The system reserves a pool of connections between System Manager and Communication Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

## Modifying the maximum number of simultaneous logins for a user

### About this task

From Release 7.1, Communication Manager allows default five simultaneous connections for a user. Use the following procedure to change the maximum number of simultaneous logins for the user.

### Procedure

1. Log on to the Communication Manager System Management interface.
2. Click **Administration > Server (Maintenance)**.
3. In the navigation pane, click **Security > Login Account Policy**.
4. In the **Login Limits** section, in the **Maximum Number of Simultaneous logins for a user** field, enter the new value.

 **Note:**

If a user is configuring  $n$  connections in System Manager for Connection Pooling, you must set the value to  $n+1$ .

5. Click **Submit**.

---

## Configure options

The Uniform Dial Plan (UDP) call type works identically with the ext call type, with an exception: if the dialed digits match the call type of UDP, Communication Manager automatically checks the UDP table to see if there is a match, regardless of the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen. If there is no match, Communication Manager then checks the local server.

If the dialed digits match the call type of ext, Communication Manager checks the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **udp-table-first**, Communication Manager checks the UDP Table first to see if there is a match. If there is no match, Communication Manager then checks the local server.

If the value in the **UDP Extension Search Order** field on the Dial Plan Parameters screen is **local-extensions-first**, Communication Manager checks the local server first to see if there is a match. If there is no match, Communication Manager then checks the UDP table.

The UDP call type allows Communication Manager to recognize strings of 14 to 18 digits, which are longer than the maximum extension length of 13 digits. However, the UDP call type can be used with any length in case this provides a useful new capability to customers.

## UDP in System Manager

You can select the Uniform Dial Plan option on the Synchronize CM Data and Configure Options page from **Elements > Communication Manager > System > Uniform Dial Plan Groups**. When you select the **Consider UDP** option, the system does not use the corresponding dial plan for the available extension range while adding an endpoint. When you do not select the **Consider UDP** option, the system uses the corresponding dial plan for the available extension range while adding an endpoint.

# Chapter 14: Managing events

---

## Managing alarms

---

### Alarming

The Alarming service provides an interface for monitoring alarms generated by System Manager and other components. You can:

- View an alarm
- Change the alarm status
- Export alarms to a Comma Separated Values (.csv) file through the Alarming service

System Manager generates alarms to notify users of system events. Alarms are classified by their effect on system operation. Alarms can also identify the system component that generate the alarm.

 **Note:**

- For Release 6.1 elements with 6.1 SAL agent and Release 6.2 elements with 6.2 serviceability agent, System Manager cannot forward traps to Network Management System (NMS). You can configure 6.1 elements with 6.1 SAL agent and 6.2 elements with 6.2 serviceability agent to directly send SNMP traps to a customer NMS.

However, for Release 6.2.x elements, you can configure the serviceability agent from System Manager instead of configuring in each element.

- For Release 5.2 and 6.0 elements, you can configure System Manager to forward alarms to Avaya Data Center (ADC).

For information on configuring serviceability agents, see Managing Serviceability Agents.

#### Related links

[Serviceability Agents](#) on page 954

---

### Cluster level alarming

From Release 7.1.3, System Manager supports cluster level alarms. Using the cluster level alarms feature, the product-specific cluster type alarms generated from one node of the cluster are cleared from another node.



 **Note:**

Cluster level alarming does not work along with alarm throttling.

## Remote key server alarms

When you configure the remote key server and if any of the remote key servers are unavailable, System Manager generates the following alarms:

| Alarm/Event ID             | Severity | Alarm description                                                               |
|----------------------------|----------|---------------------------------------------------------------------------------|
| REMOTE_KEY_SERVER_ALARM    | Major    | Disk encryption key server <IP Address of the remote key server> not reachable. |
| ALL_KEY_SERVERS_DOWN_ALARM | Major    | All configured disk encryption key servers not reachable.                       |

## Viewing alarms

### Procedure

1. On the System Manager web console, click **Services > Events > Alarms**.
2. On the Alarming page, select the alarms that you want to view.
3. Click **View**.

The Alarm - View Alarm Detail page displays the details of the selected alarms.

## Changing the alarm status

### About this task

Use this procedure to change the alarm status. Maintenance support must manually set the alarm to the required state.

The alarm status can be:

- **Raised:** Indicates the alarm is raised to notify about a system event.
- **Acknowledged:** Indicates the alarm is under investigation.
- **Cleared:** Indicates the error condition is resolved. The auto alarm clear event might result in the Cleared status.

### Procedure

1. On the System Manager web console, click **Services > Events > Alarms**.
2. On the Alarming page, select the alarm and click **Change Status**.
3. Click the status that you want to apply to the selected alarms.

---

## Exporting alarms

### About this task

You can export alarms to a Comma Separated Values (.csv) file. You can open the CSV file using a text editor such as Wordpad, or a spreadsheet application such as Microsoft Excel.

### Procedure

1. On the System Manager web console, click **Services > Events > Alarms**.
2. On the Alarming page, do one of the following:
  - To export an alarm to a CSV file, select an alarm and click **More Actions > Export Selected**.
  - To export the filtered alarms to a CSV file, click **More Actions > Export All**.

When you use **Advanced Search** or **Filter** option to filter alarms based on some criteria, **Export All** exports all the filtered data.

3. Click **Save** to save the exported file to the local disk.

---

## Deleting alarms

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Events > Alarms**.
3. On the Alarming page, perform one of the following steps:
  - To delete a specific alarm from the list, select the alarm to delete and click **More Actions > Delete Selected**.
  - To delete all the alarms from the database, click **More Actions > Delete All**.
4. Click **OK**.

---

## Filtering alarms

### About this task

The criteria for filtering the alarms are Severity, Status, Host Name, Message, Identifier, and M/E Ref Number. You can use more than one filter criteria on the selected alarms.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Events > Alarms**.

3. On the Alarming page, select the alarms you want to filter.
4. Click **Filter: Enable** at the top right corner of the Alarm List table.
5. Select the filter criteria you want to apply to the selected alarms.

The **Status** and **Severity** fields have drop down menus.

You can enter the alarm code in the Message field to find all alarms that contain a particular alarm code.

6. Click **Filter: Apply**.

 **Note:**

The system displays a message if no matching records are found to the specified filter criteria.

## Result

The system displays the alarms that match the filter criteria.

---

## Searching for alarms

### About this task

Use the Advanced Search function to find alarms based on certain specified conditions. The system displays those alarms that satisfy the search conditions. You can specify multiple search conditions.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Events > Alarms**.
3. On the Alarming page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop down fields, select the search criterion and the operator.

The default value in the first drop down field is **Time Stamp**.

5. Select or enter the search value in the third field.
6. To add another search condition, click **+** and do the following:
  - a. Select the AND or OR operator from the drop down field.
  - b. Repeat steps 4 and 5.

To delete a search condition, click **-**. You can delete a search condition if you add multiple search conditions.

7. To find alarms for the given search conditions, click **Search**.

---

## Changing the throttle period from default 720 minutes to other period for specific alarm

### About this task

You can configure the throttling period in minutes as a threshold for all alarms or alarms specific to events at spiritAgent service from Avaya Aura®. The system eliminates any redundant alarms raised within the configured period at spiritAgent service.

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Open the `AlarmThrottle.properties` file from the `$SPIRIT_HOME/config/agent` location.
3. Set `AlarmThrottlePeriod=2` in the file.

The system sets the throttle period in minutes and applies the configured period to all outgoing alarms.

4. To configure the throttle time for a specific event, open the `EPBaseRules_orig.xml` files of the specific product, which contain the events, and add the following lines:

```
<tns:ExtraAttribute>
<tns:ExtraAttributeName>alarmThrottleInterval</tns:ExtraAttributeName>
<tns:ExtraAttributeValue>2</tns:ExtraAttributeValue>
</tns:ExtraAttribute>
```

For example, for System Manager, open the `Panther_EPBaseRules_orig.xml` files.

You can apply the `alarmThrottleInterval` as the alarm throttle period for a specific event. If you do not use the generic and specific mechanisms, the system disables alarm throttling. The system sets the default alarm throttling period to 720 minutes or 12 hours. If you reconfigure the period, you must restart spiritAgent service.

5. To disable alarm throttling, perform the following steps:
  - a. In the `$SPIRIT_HOME/config/agent/AlarmThrottle.properties` file, set `AlarmThrottlePeriod=-1`.
  - b. Restart spiritAgent service.

---

## Generating test alarms

### Test alarms

You can generate a test alarm and a clear event corresponding to the generated test alarm. The severity level of the test alarm is minor. The clear event generated has no definite severity level. The clear event updates the status of the test alarms from Raised to Cleared. If Secure Access

Link (SAL) Enterprise is configured to forward alarms to Avaya Data Center (ADC), the system also forwards the test alarm and the clear event for the ADC test alarm.

### Test Alarm Event

| Test Alarm property   | Value               |
|-----------------------|---------------------|
| Alarm.Message         | Test alarm          |
| Alarm.Severity        | Minor               |
| Alarm.Status          | Raised              |
| Alarm.Log.ProcessName | TESTALARM           |
| Alarm.Log.EventCode   | TEST_ALARM_GEN_0001 |

### Test Clear Event

| Test Clear Event property | Value                      |
|---------------------------|----------------------------|
| Alarm.Message             | Clear event for test alarm |
| Alarm.Severity            | Indeterminate              |
| Alarm.Status              | Cleared                    |
| Alarm.Log.ProcessName     | TESTALARM                  |
| Alarm.Log.EventCode       | TEST_ALARM_CLR_0000        |

### Related links

[Generating the test alarm from the web console](#) on page 995

[Generating the test alarm from CLI](#) on page 996

## Generating the test alarm from the web console

### About this task

You can generate test alarms from the System Manager web console for agents, hosts, or elements installed with Serviceability Agents running version 6.3.2.4-6706-SDK-1.0 or later.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.
3. In the **Agent List** section, select one or more agents for which you want to generate alarms.
4. Click **Generate Test Alarm**.

The system generates an alarm.

5. To view the alarm, click **Events > Alarms**.

To view the alarm details, wait until the system displays the alarms on the Alarming page.

## Generating the test alarm from CLI

### Procedure

1. Log in to the computer where System Manager is installed.
2. At the command prompt, perform the following:
  - a. To check the status of spiritAgent service, type `service spiritAgent status` and press `Enter`.

The system displays `SPIRIT Agent is running`.

 **Note:**

If the system displays `SPIRIT Agent is not running`, then start spiritAgent service.

- b. To start spiritAgent service, type `service spiritAgent start` and press `Enter`.  
The `utils` directory contains spiritAgent service command line utilities.
3. To navigate to the `utils` directory, at the prompt, type `cd $SPIRIT_HOME/scripts/utils/` and press `Enter`.

4. Do one of the following:

- To generate the test alarm for System Manager, type `sh generateTestAlarm.sh` and press `Enter`.
- To generate the clear alarm for System Manager, type `sh generateTestAlarm.sh -c` and press `Enter`.
- To generate alarms on other products, repeat steps 1 to 4. You can use the **Generate Test Alarm** button on the System Manager web console Manage Serviceability Agents page for generating test alarms for all elements, including System Manager, with a click.

---

## Managing Geographic Redundancy related alarms

### Forwarding the secondary System Manager alarms to the primary System Manager server

#### Before you begin

Log on to the System Manager web console of the primary server.

#### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the left navigation pane, click **Manage Serviceability Agents > Serviceability Agents**.  
The system displays the primary and secondary System Manager entries.

3. Create a target profile of the primary System Manager server, and copy the profile to the secondary System Manager server.

The system forwards the secondary System Manager alarm to the primary System Manager server.

## Viewing the secondary System Manager alarms

### About this task

You can view the secondary System Manager alarms that are in standby mode.

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `sh $MGMT_HOME/alarmingui/scripts/DisplayAlternateDBAlarms.sh`.
3. At the prompt, type the number based on the action you want to perform.

The options are:

- (0) Exit
- (1) Display All Alarm count
- (2) Display alarm by notification oid (0)
- (3) Display alarm by Status (0)
- (4) Clear Alarm with notification oid (0)
- (5) Display all alarms
- (6) Display Alarms by severity (0)

System Manager displays the alarms according to your selected option.

---

## AutoRefresh Alarm List field descriptions

The Alarming page displays a list of alarms. Use this page to view the alarms in the **Auto-Refresh** mode. In this mode, the page updates the alarm information automatically.

| Name       | Description                                    |
|------------|------------------------------------------------|
| Time Stamp | The date and time when the alarm is generated. |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Severity</b>              | <p>The severity of the alarm. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Cleared:</b> Displayed as a status change for a raised alarm after the issue is rectified.</li> <li>• <b>Critical:</b> Displayed in red is for critical failures that cause system or services to be non-functional and require immediate resolution and fix.</li> <li>• <b>Major:</b> Displayed in orange is for failures that cause critical degradation of service and require immediate attention.</li> <li>• <b>Minor:</b> Displayed in yellow is for failures that: <ul style="list-style-type: none"> <li>- Cause degradation of service, but continue to support a crucial part of the system.</li> <li>- Require action, but the consequences of the failure are gradual.</li> <li>- Interfere with a feature or impair the services to trunks or stations.</li> </ul> </li> <li>• <b>Warning:</b> Displayed in purple is for failures that do not cause significant degradation of service. This alarm is not reported to the attendant console or Initialization and Administration System (INADS).</li> <li>• <b>Indeterminate:</b> Displayed in blue is for an alarm that does not have any rules defined in the System Manager. It is displayed as a raw SNMP packet as there is no information available in the System Manager for its description and severity. Hence, marked as <b>Indeterminate</b>.</li> </ul> |
| <b>Status</b>                | The current status of the alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Host Name/SysName</b>     | The name of the host computer that generated the alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Source IP address</b>     | The IP address of the system that generated the alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>           | A detailed description of the problem that generated the alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Identifier</b>            | The unique identifier for an alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Event ID</b>              | The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>NotificationOID</b>       | The SNMP OID of the alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>M/E Ref Number/SysOID</b> | <p>The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm.</p> <p>For alarms that are generated from the trap listener service, the system displays the System OID.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Button                    | Description                                                                                                               |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Alarm landing Page</b> | Changes the mode from <b>Auto-Refresh</b> to Manual refresh and displays the Alarming home page. This is a toggle button. |



## Alarming field descriptions

| Name                           | Description                                                                                                                                                                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Stamp</b>              | The date and time when the alarm is generated.                                                                                                                                                                                                                          |
| <b>Severity</b>                | The severity of the alarm.                                                                                                                                                                                                                                              |
| <b>Status</b>                  | The current status of the alarm.                                                                                                                                                                                                                                        |
| <b>Host Name/SysName</b>       | The name of the host server that generated the alarm.<br>For the trap listener service, this column displays the system name.                                                                                                                                           |
| <b>Source IP Address</b>       | The IP address of the system that generated the alarm.                                                                                                                                                                                                                  |
| <b>Description</b>             | A detailed description of the problem that generated the alarm.                                                                                                                                                                                                         |
| <b>M/E Ref Number / SysOID</b> | The unique identification number assigned to the product, also called the product ID. This number helps in identifying the component that generated the alarm.<br><br>For alarms that are generated from the trap listener service, the system displays the System OID. |
| <b>Identifier</b>              | The unique identifier for an alarm.                                                                                                                                                                                                                                     |
| <b>Event ID</b>                | The log event ID if the alarm is generated from logs or the Event OID if the alarm is generated from the trap listener service.                                                                                                                                         |
| <b>NotificationOID</b>         | The SNMP OID of the alarm.                                                                                                                                                                                                                                              |

| Button                                   | Description                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View</b>                              | Displays the details of the selected alarms.                                                                                                                                                                                                                                                                                                                         |
| <b>Change Status</b>                     | Changes the status of the selected alarm. The options are: <ul style="list-style-type: none"> <li>• <b>Raised</b></li> <li>• <b>Cleared</b></li> <li>• <b>Acknowledged</b></li> </ul>                                                                                                                                                                                |
| <b>Auto-Refresh Mode</b>                 | Changes over to the <b>Auto-Refresh</b> mode. When the Alarming page is set in this mode, it automatically updates the alarms in the table. This is a toggle button.                                                                                                                                                                                                 |
| <b>More Actions &gt; Export Selected</b> | Exports the selected alarms to a CSV file. You can view the logs using the Wordpad or Excel application.                                                                                                                                                                                                                                                             |
| <b>More Actions &gt; Export All</b>      | Exports all the alarms to a CSV file. You can view the logs using the Wordpad or Excel application.<br><br> <b>Note:</b><br>When you use <b>Advanced Search</b> or <b>Filter</b> option to filter alarms based on some criteria, <b>Export All</b> exports all the filtered data. |
| <b>More Actions &gt; Delete Selected</b> | Deletes the alarms that you select from the list.                                                                                                                                                                                                                                                                                                                    |

*Table continues...*

| Button                              | Description                                                                                            |
|-------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>More Actions &gt; Delete ALL</b> | Deletes all alarms that the system displays on the page.                                               |
| <b>Advanced Search</b>              | Displays fields that you can use to specify the search criteria to search for an alarm.                |
| <b>Refresh</b>                      | Refreshes the log information in the table.                                                            |
| <b>Filter: Enable</b>               | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>              | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Clear</b>                | Clears the filter criteria.                                                                            |
| <b>Filter: Apply</b>                | Filters alarms based on the filter criteria.                                                           |
| <b>All</b>                          | Selects all the alarms in the table.                                                                   |
| <b>None</b>                         | Clears the check box selections.                                                                       |
| <b>Previous</b>                     | Displays the logs in the previous page. This button is not available if you are on the first page.     |
| <b>Next</b>                         | Displays the logs in the next page. This button is not available if you are on the last page.          |

### Criteria section

This system displays the section when you click **Advanced Search** on the top-right corner of the page.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>Use this section to specify search conditions. Select the search criteria from the first drop down list. Select the operator from the second drop down list. Enter the search value in the text field.</p> <p>Select the following search criteria from the first drop down list:</p> <ul style="list-style-type: none"> <li>• Time Stamp: Searches all alarms that match the specified date and time. The valid format for entering the date is MM/DD/YYYY. The valid format for entering the time is HH:MM.</li> <li>• Severity: Searches all alarms that match the specified severity level.</li> <li>• Status: Searches all alarms that match the specified status.</li> <li>• Host Name: Searches all alarms that are generated from the specified host.</li> <li>• M/E Ref Number: Searches all alarms that match the specified M/E Ref Number.</li> <li>• Event ID: Searches all alarms that match the specified Event ID.</li> <li>• Source IP address: Searches all alarms that are generated from the specified source IP address.</li> <li>• NotificationID: Searches all alarms that match the specified NotificationID.</li> <li>• Identifier: Searches all alarms that match the specified identifier.</li> <li>• Description: Searches all alarms that match the specified description.</li> </ul> <p>The operators available are based on the search criterion that you select in the first drop down field. The following operators are available for search criteria:</p> <ul style="list-style-type: none"> <li>• Time Stamp: =, &gt;, &lt;, &gt;=, &lt;=, &gt;=, !=</li> <li>• Severity: Equals, Not Equals</li> <li>• Status: Equals, Not Equals</li> <li>• Host Name: Equals, Not Equals, Starts With, Ends With, and Contains</li> <li>• Identifier: =, &gt;, &lt;, &gt;=, &lt;=, &gt;=, !=</li> <li>• Source IP address: Equals, Not Equals, Starts With, Ends With, and Contains</li> <li>• Event ID: Equals, Not Equals, Starts With, Ends With, and Contains</li> <li>• Description: Equals, Not Equals, Starts With, Ends With, and Contains</li> <li>• M/E Ref Number: Equals, Not Equals, Starts With, Ends With, and Contains</li> </ul> <p>When you select <b>Begin Date</b> and <b>End Date</b> from the first drop down list, you are prompted to enter the date in the third field.</p> |

| Button                       | Description                                                              |
|------------------------------|--------------------------------------------------------------------------|
| <b>Clear</b>                 | Clears the entered search criteria and sets the default search criteria. |
| <b>Search</b>                | Searches the alarms based on the search conditions.                      |
| <b>Close/Advanced Search</b> | Hides the search fields.                                                 |
| <b>+</b>                     | Adds a search condition.                                                 |
| <b>-</b>                     | Deletes a search condition.                                              |

---

## Managing logs

---

### Logging service

The Logging service provides configuration capabilities and overall management of logs. It receives and stores log events and harvests file-based logs or local database logs. You can view and monitor logs and their details through the log viewer using the System Manager Web Console. The log viewer is integrated with the common console to provide a consistent presentation of log messages for System Manager and the adopters.

The log viewer displays a list of logs where you can view each log details, perform a search for logs, and filter specific logs. The log details include event information that generates the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

The following are some of the log types:

- Security: Security loggers gather security logs.
- Audit: Audit loggers gather audit logs.
- Operation: Operational loggers gather operational logs.
- Debug: Debug loggers collect debug information to troubleshoot issues at the customer site.

The Logs menu in System Manager comprises:

- Log Harvester: Through the Log Harvester menu, you can harvest log files for one or more products of the same or different types, running on the same or different computers.
- Log Settings: This menu displays the loggers and appenders for the selected log configuration file. You can modify the logger and appender settings through this menu.
- Log Viewer: The log viewer allows you to view the logs generated by System Manager and other components and their details. You can view details of each log, perform a search for logs, and filter specific logs.

---

## Log Types

The following are some of the log types you may come across when viewing logs on the System Manager Web Console. You can view the station-specific logs in the `/var/log/Avaya/mgmt/iptcm` directory.

### **Security**

Security loggers gather security logs.

### **Audit**

Audit loggers gather audit logs.

### **Operation**

Operational loggers gather operational logs.

### **Debug**

Debug loggers collect debug information to troubleshoot issues at the customer site. These loggers are categorized based on the Communication System Management components.

#### **Debug.Station**

Debug Station loggers gather debug information for station management related operations.

#### **Debug.Template**

Template Debug loggers gather debug information for template management related operations.

#### **Debug.CM**

CM debug loggers gather debug information for communication between Communication Manager and the Communication System Management server.

#### **Debug.NCM**

NCM debug logger gathers debug information related to Element Cut Through.

#### **Debug.Synch**

Synch debug logger gathers debug information for synchronization operations.

#### **Debug.Model**

Model debug logger gathers debug information for database operations.

### **Debug**

Debug logger gathers debug information other than those gathered for the debug types mentioned above.

---

## Managing log harvester

### Log harvester

The log harvesting service manages the retrieval, archival, and analysis of the harvested log files stored in Serviceability Agent enabled hosts or elements. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging Service through HTTPS. With a successful harvest request related to a harvest profile, the logging service accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same or different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface, and the status of each archive is available in the user interface table.

You can perform the following operations using the log harvesting service:

- Create a log harvesting profile to specify the products for which you want to harvest the logs.
- Submit the log harvesting request defined in a profile to the product.
- View the status of the log harvesting request.
- Store the harvested log files of a product in an archive file.
- View the harvested log files stored in the archive file.
- Download the harvested log files to a local computer.
- Search for a matching text in the harvested log files.

### Accessing the Log Harvester service

#### Procedure

On the System Manager web console, click **Services > Events > Logs > Log Harvester**.

### Creating a new log harvesting profile

#### About this task

To harvest log files for products running on different servers, you must specify multiple filter criteria.

#### Before you begin

To create a new log harvesting profile, you must specify:

- The hostname of the server on which the product is running.

If you do not see the hostname of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command:

```
cd /opt/nortel/oam-logging
./configureSpiritAgentClient.sh <enrollment password>
```

The system now enrolls CS 1000 to the log harvester of System Manager.

- The product name
- The directories or the log files
- The filter text if you select one or more directories

 **Note:**

By default, harvesting is enabled for System Manager. All other products should always integrate and install their log harvesting extension packs during System Manager installation. After integration, they directly get their product type and files in System Manager in the drop down list on the Log Harvesting page.

## Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, click **New**.
3. On the Create New Profile page, do the following:
  - a. In **Profile Name**, type the profile name.
  - b. In **Profile Description**, type a description of the profile.
4. Select the hostname of the server, product, and directories or files from the respective fields.
  - To select multiple directories or files from the respective list boxes, press **CTRL** and click the directories or files.
  - To clear a selection, press **CTRL** and click the item.
  - To add another log harvesting request for a different product, or another instance of the same product running on the same server or a different server, click plus (+).
5. **(Optional)** If you select one or more directories, in the **File Name Filter** field, type a text pattern as the filter criteria.  
  
During the harvesting operation, the system harvests those files that match the filter criteria.
6. Click **Save Profile** to save the profile and the log harvesting requests in the profile.

## Related links

[Create New Profile field descriptions](#) on page 1012

## Editing a log harvesting profile

### Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, select a profile, and click **Edit**.
3. On the Harvest Criteria Edit page, modify the information in the **Profile Name** and **Profile Description** fields.

4. Modify the host name of the server, product, and directories or files from the respective fields.
  - To select multiple directories or files from the respective list boxes, press **CTRL** and click the directories or files.
  - To clear a selection, press **CTRL** and click the item.
  - To add another log harvesting request for a different product, or another instance of the same product running on the same server or a different server, click plus (+).
5. **(Optional)** If you select one or more directories, in the **File Name Filter** field, type a text pattern as the filter criteria.

During the harvesting operation, the system harvests those files that match the filter criteria.
6. Click **Save Profile** to save the changes to the log harvesting profile.

#### Related links

[Harvest Criteria Edit field descriptions](#) on page 1013

## Viewing details of a log harvesting profile

### Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, select a profile, and click **View**.

The Profile Criteria View page displays the details of the selected log harvesting profile.
3. Click **Done**.

#### Related links

[Profile Criteria View field descriptions](#) on page 1013

## Viewing the harvested log files in an archive

### About this task

Use this procedure to view the harvested log files of a product stored in an archive file.

### Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
3. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.
4. Click **Show Files**.
5. On the Search Archives page, navigate through the folders to view the harvested log files.



## Deleting log harvest profiles

### About this task

You cannot delete profiles that are in use by the Log Harvester service. If you attempt to delete profiles that are in use, System Manager displays an error message.

### Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, select a profile, and click **Delete**.
3. On the Profile Delete Confirmation page, click **Delete**.

System Manager deletes all requests and archives related to the profile from the file system.

## Submitting a request for harvesting log files

### About this task

Use this feature to submit a log harvesting request to one or more products running on the same or different servers. After the request is successfully processed, the system on which the products are installed returns the harvested log files specified in the request. When you select a profile and click **Request**, the system generates a single request for all the requests contained in the profile.

### Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
3. On the Harvest Archives page, type the relevant information in the **Archive Name** and **Archive Description** fields.

The system saves the harvested log files in the specified archive file.

4. Click **Run Profile** to send a request.

The table in the Harvest Criteria View section provides you the log harvesting request status. If the execution status of the request is successful, the system creates a zip file containing the harvested log files and saves the file in the specified location.

### Related links

[Harvest Archives field descriptions](#) on page 1014

## Viewing details of a log harvesting request

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
4. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.

5. If the system does not display any requests, submit a new request.
6. Click **View**.

The Harvest - View Harvest detail page displays the details of the selected request.

#### Related links

[Harvest - View Harvest detail field descriptions](#) on page 1015

## Searching for text in a log file

Use this feature to search for matching text in the product log file.

### About this task

The search is based on Lucene Search. The search results are highlighted as per the Lucene highlighter. The highlight package contains classes to provide keyword in context features, typically used for highlighting search terms on the results page.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
4. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.
5. Click **Show Files**.
6. On the Search Archives page, in the **Enter search text** field, enter the text for which you want to search.
7. In the Tree view, navigate to the log file by expanding the folders and select the log file.
8. Click **Search**.

The system displays the search results in the Search Result Panel. The **Search Results Panel** field displays the line numbers as hyperlinks on which the searched text is found.

9. Click the hyperlink in the **Search Results Panel** field.

The system displays the page that contains the highlighted searched text in the **Log Browser Panel** field.

#### Related links

[Search Archives field descriptions](#) on page 1015

## Viewing the contents of harvested log files

### About this task

Use this feature to view the log messages stored in the harvested log files for a product. You can view the contents of one log file at a time.

## Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
4. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.

The system lists the harvested log files.

7. Select the log file and click **View**.

The system displays the file content in the Log Browser Panel pane.

## Related links

[Search Archives field descriptions](#) on page 1015

## Downloading the harvested log files

### About this task

You can download the harvested log files of one or more products stored in a zip file on the local server.

## Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
4. On the Harvest Archives page, in the Harvest Request Details section, click a request in the table.
5. If the system does not display any requests, submit a new request.
6. Click **Show Files**.
7. On the Search Archives page, select a product name, host name of the server on which one or more products are running, or a directory.
  - If you select a product name, the system creates a zip file that contains the harvested log files for the selected product instances running on the same server or different servers.
  - If you select a host name of a server under a product, the system creates a zip file containing the harvested log files for the products running on the selected server.
  - If you select a directory, the system creates a zip file containing the harvested log files under the selected directory.

8. Click **Download**.

The system prompts you to save the file on your local server.

9. Click **Save**.

### Related links

[Search Archives field descriptions](#) on page 1015

## Filtering log harvesting profiles

Use this feature to set filter criteria to view those log harvesting profiles that meet the set filter criteria. The titles of the table columns displaying the log harvesting profiles are the filter criteria.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Harvester**.
3. On the Log Harvester page, click **Filter: Enable**.

You can find this button at the top right of the table containing log harvesting profiles.

4. Enter or select the filter criteria.

You can filter the log harvesting profiles by the name, description, and creator of the profiles.

5. Click **Filter: Apply**.

#### **Note:**

If no records matching the filter criteria are found, the Log Harvester page displays a message that no records matching the search criteria are found.

The log harvesting profile table displays the profiles that match the specified filter criteria.

## Filtering log harvesting requests

Use this feature to set filter criteria to view those log harvesting requests that meet criteria. The titles of the columns of the table that displays the log harvesting requests are the filter criteria.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Harvester**.
3. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
4. On the Harvest Archives page, click **Filter: Enable**.
5. Enter or select the filter criteria.

You can filter the log harvesting requests by:

- The request ID of the log harvesting request. For example, to view the requests starting with Request ID 5, enter 5.

- The zip file name that stores the harvested files.
- The description of the log harvesting request.
- The location of the archived file that stores the harvested files.
- The status of the log harvesting request.
- The description of the log harvesting request status.

6. Click **Filter: Apply**.

 **Note:**

If no records matching the filter criteria are found, the Log Harvesting page displays a message that no records matching the search criteria are found.

The table containing log harvesting requests displays those log harvesting requests that match the specified filter criteria.

## Log Harvester field descriptions

This page displays the list of log harvest profiles created in System Manager. You can use buttons on this page to perform the following operations:

- View and edit the details of a selected log harvest profile.
- Delete a profile.
- Add a new log harvest profile.
- View the details of log harvest requests for a profile.

| Name                      | Description                                     |
|---------------------------|-------------------------------------------------|
| <b>Profile Name</b>       | The name of the log harvesting profile.         |
| <b>Description</b>        | A brief description of the profile.             |
| <b>Created By</b>         | The name of the creator of the profile.         |
| <b>Created Time Stamp</b> | The date and time when the profile was created. |

| Button          | Description                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------|
| <b>View</b>     | Displays the Harvest Archives page. You can use this page to view the details of a selected log harvest profile.    |
| <b>New</b>      | Displays the Create New Profile page. You can use this page to create a new log harvesting profile.                 |
| <b>Edit</b>     | Displays the Edit Profile page. You can use this page to edit a log harvesting profile.                             |
| <b>Delete</b>   | Deletes the selected profile. You cannot delete a profile if the profile is in use by the Log Harvester service.    |
| <b>Requests</b> | Displays the Harvest Archives page. You can use this page to run the log harvesting requests in a selected profile. |

*Table continues...*

| Button                 | Description                                                                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter: Disable</b> | Hides the fields displayed under the columns to apply the filters without resetting the filter criteria. This is a toggle button.                                                                                                                |
| <b>Filter: Enable</b>  | Enables the filter and displays the fields under the columns in the table where you can enter the filter criteria. Only the columns on which you can apply the filter, display where you can enter the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters the log harvest profiles present in the system based on the filter criteria.                                                                                                                                                             |

## Create New Profile field descriptions

Use this page to create a new log harvesting profile for harvesting log messages from the log files for one or more products. The files can reside on one or more servers.

| Name                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>        | The name of the log harvesting profile.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Profile Description</b> | A brief description of the profile. This is an optional field.                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Host Name</b>           | <p>The host name of the servers on which products are installed.</p> <p>If you do not see the hostname of CS 1000 when you create the profile, at the command prompt of CS 1000, run the following command:</p> <pre>cd /opt/nortel/oam-logging ./configureSpiritAgentClient.sh &lt;enrollment password&gt;</pre> <p>After typing a minimum of three characters, wait for three seconds to capture the final keyword and fetch the required results.</p> |
| <b>Product</b>             | The products for which you can harvest logs.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Directories</b>         | A list of directories that contain the log files for the selected product.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Files</b>               | The log files that you can harvest for the selected product.                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Filter Text</b>         | <p>The text, based on which, the system filters the log files present in the selected directory for harvesting.</p> <p>When you select the <code>/a/b/c</code> directory and type <code>com</code> in this field, the harvest operation for this profile harvests the log files in the directory <code>/a/b/c</code>. The log files contain <code>com</code> in the file name. The field does not support wild cards.</p>                                |

| Button              | Description                                                                     |
|---------------------|---------------------------------------------------------------------------------|
| <b>+</b>            | Displays another log harvesting request for a product.                          |
| <b>-</b>            | Deletes the log harvesting request for the product.                             |
| <b>Commit</b>       | Commits the filter criteria for the selected directories.                       |
| <b>Save Profile</b> | Saves the new profile and settings for log harvesting requests in the database. |

## Harvest Criteria Edit field descriptions

Use this page to edit an existing log harvesting profile.

| Name                           | Description                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>            | Displays the name of the log harvesting profile.                                                                                                                                                                                                                                                                                                                                                |
| <b>Profile Description</b>     | Displays a brief description of the profile.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Host Name</b>               | Displays the hostname of the servers on which you install the products.                                                                                                                                                                                                                                                                                                                         |
| <b>Product</b>                 | Displays the products for which you can harvest logs.                                                                                                                                                                                                                                                                                                                                           |
| <b>Directories/Filter Text</b> | Lists the directories containing the log files for the selected product.                                                                                                                                                                                                                                                                                                                        |
| <b>Files</b>                   | Displays the log files that you can harvest for the selected product.                                                                                                                                                                                                                                                                                                                           |
| <b>Filter Text</b>             | <p>Displays the text, based on which, the log files present under a selected directory gets filtered for harvesting.</p> <p>If you select the directory <code>/a/b/c</code> and enter <code>com</code> in the <b>Filter Text</b> field, the harvest operation for this profile harvests the log files that contain <code>com</code> in the file name. The field does not support wildcards.</p> |

| Button              | Description                                                                                           |
|---------------------|-------------------------------------------------------------------------------------------------------|
| <b>+</b>            | Allows you to specify another log harvesting request for a product.                                   |
| <b>-</b>            | Deletes the log harvesting request for the product.                                                   |
| <b>Commit</b>       | Commits the filter criteria for the selected directories.                                             |
| <b>Save Profile</b> | Saves the new profile and settings for log harvesting requests in the database.                       |
| <b>Cancel</b>       | Ignores the changes you make to the Harvest Criteria Edit page and returns to the Log Harvester page. |

## Profile Criteria View field descriptions

Use this page to view the details of a selected log harvest profile.

| Name                       | Description                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>        | Displays the name of the log harvesting profile.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Profile Description</b> | Displays a brief description of the profile.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Product</b>             | Displays the name of the product for which logs are harvested.                                                                                                                                                                                                                                                                                                                                     |
| <b>Hosts</b>               | Displays the hostname of the server on which the product resides.                                                                                                                                                                                                                                                                                                                                  |
| <b>Files</b>               | Displays the names of the log files for which you can harvest log messages.                                                                                                                                                                                                                                                                                                                        |
| <b>Directory</b>           | Displays the directory that contains the log files.                                                                                                                                                                                                                                                                                                                                                |
| <b>Filter Text</b>         | <p>Displays the text, based on which, the log files present under a selected directory are filtered for harvesting. For example, if you select the directory <code>/a/b/c</code> and enter the text <code>com</code> in this field, the harvest operation for this profile harvests the log files that contain <code>com</code> in the file name. This field does not support wild characters.</p> |

| Button  | Description                                                    |
|---------|----------------------------------------------------------------|
| Done    | Closes this page and returns to the Harvest Profile List page. |
| Refresh | Refreshes the records in the table.                            |

## Harvest Archives field descriptions

Use this page to create an archive for the log harvesting request. The archive created for a successful harvesting request contains the requested log files in a compressed file.

| Name                | Description                                                             |
|---------------------|-------------------------------------------------------------------------|
| Archive Name        | The name of the archive file to create for storing harvested log files. |
| Archive Description | A brief description of the archive. This field is optional.             |

| Name                | Description                                                                                                                                                                                                                                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Request Id          | The unique identification number assigned to a log harvesting request.                                                                                                                                                                                                                                                                            |
| Archive Name        | The name of the archive file for storing harvested log files.                                                                                                                                                                                                                                                                                     |
| Request Time Stamp  | The date and time when the log harvesting request is submitted.                                                                                                                                                                                                                                                                                   |
| Request Description | A brief description of log harvesting requests.                                                                                                                                                                                                                                                                                                   |
| Status              | The status of log harvesting requests. The options are: <ul style="list-style-type: none"> <li>• SUCCESS: System Manager successfully harvests the log messages.</li> <li>• FAILURE: System Manager fails to harvest the log messages for the product.</li> <li>• PARTIAL SUCCESS: System Manager partially harvests the log messages.</li> </ul> |
| Status Time Stamp   | The date and time when the execution status of the log harvesting request is generated.                                                                                                                                                                                                                                                           |
| Status Description  | A brief description of the log harvesting request status. The description contains information about the success or failure of the log harvesting request.                                                                                                                                                                                        |
| Location            | The location where the harvested log messages are archived.                                                                                                                                                                                                                                                                                       |

| Button      | Description                                                                                                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Run Profile | Runs log harvesting requests for selected profiles.                                                                                                                                                                                                                                        |
| View        | Displays the View Harvest detail page to view the details of selected log harvesting requests.                                                                                                                                                                                             |
| Show Files  | Displays the Search Archives page to: <ul style="list-style-type: none"> <li>• Search for text contained in the harvested log files.</li> <li>• Download log files of one or more products running on the same or different servers.</li> <li>• View the contents of log files.</li> </ul> |

*Table continues...*



| Button                 | Description                                                                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter: Disable</b> | Hides the fields displayed under the column filter fields without resetting the filter criteria. This is a toggle button.                                                                                                                                       |
| <b>Filter: Enable</b>  | Displays fields under the column headers of the table that displays the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields to enter the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters the log harvest profiles in the system based on the filter criteria.                                                                                                                                                                                    |

## Search Archives field descriptions

Use this page to perform the following activities on the log files contained in an archive:

- View the contents of the harvested log files.
- Search a text in the harvested log files.
- Download the harvested log files on your local server.

| Name                        | Description                                                                                                                                                                                                                                                      |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enter search text</b>    | The text that you want to search for in the harvested log files.                                                                                                                                                                                                 |
| <b>List box</b>             | Displays the hierarchy of the harvested log files in an archive. The files are organized in a tree view.                                                                                                                                                         |
| <b>Log Browser Panel</b>    | Displays the contents of the selected log files.                                                                                                                                                                                                                 |
| <b>Search Results Panel</b> | Displays the search results. This field displays the line numbers as hyperlinks in which the searched text is found. When you click the line number, the system displays the line containing the searched text at the top in the <b>Log Browser Panel</b> field. |

| Button          | Description                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Previous</b> | Displays the log file contents on the previous page. This button is available if the contents of log files span across multiple pages. |
| <b>Next</b>     | Displays the log file contents on the next page. This button is available if the contents of log files span across multiple pages.     |
| <b>Search</b>   | Searches for the text occurrences specified in the <b>Enter search text</b> field in the selected log files.                           |
| <b>View</b>     | Displays the contents of the selected log files in the <b>Log Browser Panel</b> field.                                                 |
| <b>Download</b> | Downloads the selected log files present in the archive to your local server.                                                          |

## Harvest - View Harvest detail field descriptions

Use this page to view the details of a selected log harvest request.

**View Parent**

| Name                       | Description                                                                                                                                                                                                                                                                              |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Request Id</b>          | Displays the unique identification number assigned to a log harvesting request.                                                                                                                                                                                                          |
| <b>Archive Name</b>        | Displays the name of the archive file that stores the harvested log files containing the log messages.                                                                                                                                                                                   |
| <b>Status</b>              | Displays the status of log harvesting requests. The options are: <ul style="list-style-type: none"> <li>• <b>SUCCESS</b>: System Manager successfully harvests the log messages.</li> <li>• <b>FAILURE</b>: System Manager fails to harvest the log messages for the product.</li> </ul> |
| <b>Request Description</b> | Displays a brief description of the log harvesting request.                                                                                                                                                                                                                              |

**Child Request Details**

| Name                      | Description                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Product</b>            | Displays the unique identification number assigned to a log harvesting request.                                                                                                                                                                                                             |
| <b>Status</b>             | Displays the status of the log harvesting request. The options are: <ul style="list-style-type: none"> <li>• <b>SUCCESS</b>: System Manager successfully harvests the log messages.</li> <li>• <b>FAILURE</b>: System Manager fails to harvest the log messages for the product.</li> </ul> |
| <b>Host Name</b>          | Displays the hostname of the server on which the product resides.                                                                                                                                                                                                                           |
| <b>Status Description</b> | Displays a brief description of the execution status of the request.                                                                                                                                                                                                                        |
| <b>Status Time Stamp</b>  | Displays the date and time when the system generates the status of the log harvesting request.                                                                                                                                                                                              |

| Button                 | Description                                                                                                                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Done</b>            | Closes this page and returns to the Harvest Archives page.                                                                                                                                                                                                   |
| <b>Refresh</b>         | Refreshes the records in the table.                                                                                                                                                                                                                          |
| <b>Filter: Enable</b>  | Displays fields under the column headers of the table displaying the log harvesting requests. You can enter the filter criteria in these fields. Only columns that can be filtered display the fields to enter the filter criteria. This is a toggle button. |
| <b>Filter: Apply</b>   | Filters the log harvesting requests based on the filter criteria.                                                                                                                                                                                            |
| <b>Filter: Disable</b> | Hides the fields displayed under the columns to apply the filters without resetting the filter criteria. This is a toggle button.                                                                                                                            |

## Managing log settings

### Log Settings

Log Settings displays the loggers and appenders for any log configuration file that you select. You can also modify the logger and appender settings through this menu. The Logger List displays the name and level of the log along with the appender details.

### Accessing the Log Settings service

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Settings**.

#### Result

The System Manager displays the **Log Settings** page.

### Viewing loggers for a log file

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.

#### Related links

[Logging Settings field descriptions](#) on page 1017

### Logging Settings field descriptions

Use this page to view and edit loggers defined in a log file.

#### Log Settings

| Name        | Description                                           |
|-------------|-------------------------------------------------------|
| Logger List | The field lists the log files that you can configure. |

#### Logger List

| Name                      | Description                                            |
|---------------------------|--------------------------------------------------------|
| Logger                    | The loggers in the selected log files.                 |
| Log level                 | The level of logging set for the corresponding logger. |
| Attached Appenders > Name | The name of the appender.                              |

*Table continues...*

| Name                                     | Description                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Attached Appenders &gt; File Path</b> | The path of the file to which the appender logs the information.                      |
| <b>Attached Appenders &gt; Facility</b>  | The process running on the machine that created the log message.                      |
| <b>Attached Appenders &gt; host</b>      | The name of the syslog host where the log output is stored.                           |
| <b>Show All</b>                          | An option to select the maximum number of logger records that you can view at a time. |

| Button      | Description                                                     |
|-------------|-----------------------------------------------------------------|
| <b>Edit</b> | Displays the Edit Logger page that you can use to edit loggers. |

### Related links

[Viewing loggers for a log file](#) on page 1017

## Editing a logger in a log file

### About this task

You can set log levels for loggers defining the level of logging the logger logs.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
4. In the **Logger List** section, select a logger, and click **Edit**.
5. On the Edit logger page, in the **Log Level** field, select a log level.
6. To view the logs for successful events, click **Info** in the **Log Level** of the specified log.

For example, as a user of System Manager Communication Manager capabilities, if you set the **Log Level** to **Info** in `com.avaya.ipbcm.eps.logging.audit` and `com.avaya.ipbcm.eps.logging.operation`, the system captures the successful events in the audit log and the operational log present at `/var/log/Avaya/mgmt/ipbcm/audit.log` and `/var/log/Avaya/mgmt/ipbcm/operation.log` respectively.

#### **Note:**

If you perform an application upgrade, the system does not retain the modified log level configuration. After an application upgrade, you must configure the log level settings again to view the logs for successful events.

7. Click **Commit**.

The log level is set for the selected logger.

## Related links

[Edit Logger field descriptions](#) on page 1020

## Forwarding System Manager syslog messages to remote server Procedure

1. On a remote machine where syslog server is running, do the following:
  - a. Open the `rsyslog.conf` file, and remove the comment for the following lines:

```
$ModLoad imudp
$UDPServerRun 514
```

- b. Restart the rsyslog service.

The system accepts UDP messages on the default port 514.

2. To configure security audit logs for the syslog server, do the following:
  - a. On the System Manager web console, click **Services > Events**.
  - b. In the left navigation pane, click **Logs > Log settings**.
  - c. On the Log Settings page, in the **Logger** column, select **com.avaya.security.iam.audit**.
  - d. Click **Edit**.
  - e. On the Edit Logger page, click **Attach**.
  - f. On the Attach Appender page, in the **Select Appender** field, select **SYSLOG**.
  - g. Click **Commit**.

Add SYSLOG as an appender for the audit log.
3. To modify the syslog configuration on System Manager, do the following:
  - a. Select the SYSLOG appender and click **Edit**.
  - b. Change the host and provide the IP address of the remote server where the rsyslog service runs on UDP with port 514.

## Assigning an appender to a logger

### About this task

The appender where a logger logs the messages.

### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
4. In the **Logger List** section, select a logger, and click **Edit**.
5. On the Edit logger page, click **Attach** in the Attached Appendors section.

6. On the Attach Appender page, select an appender in the **Select Appender** field.
7. Click **Commit**.

The appender is added to the selected logger, and you can view the appender on the **Log Settings** page.

#### Related links

[Attach Appender field descriptions](#) on page 1022

### Modifying an appender

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
4. In the **Logger List** section, select a logger, and click **Edit**.
5. On the Edit logger page, in the **Attached Appendors** section, select an appender.
6. Click **Edit**.
7. On the Edit Appender page, modify the appender information.

You can modify information in the **Threshold Log Level**, **Rotate File Size**, **File Path**, **Max Retention File Size**, and **Max Retention Time** fields.

8. Click **Commit**.

#### Related links

[Edit Appender field descriptions](#) on page 1021

### Removing an appender from a logger

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Settings**.
3. On the Log Settings page, in the **Logger List**, click a log file.
4. In the **Logger List** section, select a logger, and click **Edit**.
5. On the Edit logger page, select an appender in the **Attached Appendors** section.
6. Click **Detach**.

### Edit Logger field descriptions

Use this page to edit logger and appender information. You can also add and remove appenders from the loggers.

## Logger

| Name             | Description                                          |
|------------------|------------------------------------------------------|
| <b>Logger</b>    | The name of the logger.                              |
| <b>Log level</b> | The level for which the logger logs the information. |

## Attached Appenders

| Name                           | Description                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Appender</b>                | The name of the appender.                                                                                                                                |
| <b>Threshold Log Level</b>     | The threshold log level set for the appender. Appender logs information of log type set in the threshold log level.                                      |
| <b>File Path</b>               | The path of the file where the appender logs the information.                                                                                            |
| <b>Rotate File Size</b>        | The file size for rotation of the log file.<br>The file size unit can be in KB or MB.<br>The value for the file size must be from 1 through 100MB.       |
| <b>Max Retention File Size</b> | The maximum retention file size for the log file.<br>The file size unit can be in KB or MB.<br>The value for the file size must be from 1 through 100MB. |
| <b>Max Retention Time</b>      | The maximum retention time for the log file.<br>The value for the retention time must be from 1 through 180 days.                                        |
| <b>Facility</b>                | The process running on the machine for which log messages are created.                                                                                   |
| <b>Host</b>                    | The name of the syslog host that stores the log output.                                                                                                  |
| <b>Header</b>                  | The header part of the syslog packet. The header part contains the timestamp and host name information.                                                  |
| <b>Facility Printing</b>       | The printed message includes the facility name of the application.                                                                                       |

| Button        | Description                                                                        |
|---------------|------------------------------------------------------------------------------------|
| <b>Edit</b>   | Displays the Edit Appender page. Use this page to modify the appender information. |
| <b>Attach</b> | Displays the Attach Appender page. Use this page to add an appender to the logger. |
| <b>Detach</b> | Removes the selected appender from the logger.                                     |
| <b>Commit</b> | Saves the changes in the logger information to the database.                       |
| <b>Cancel</b> | Closes the Edit Logger page and returns you to the Logging Configuration page.     |

## Edit Appender field descriptions

Use this page to edit the information of an appender.

| Name                           | Description                                                                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Logger</b>                  | The name of the logger.<br> <b>Note:</b><br>You can view this information.   |
| <b>Appender</b>                | The name of the appender.<br> <b>Note:</b><br>You can view this information. |
| <b>Threshold Log Level</b>     | The threshold log level set for the appender. Appender logs information of log type set in the threshold log level.                                           |
| <b>Rotate File Size</b>        | The file size for rotation of the log file.<br>The file size unit can be in KB or MB.<br>The value for the file size must be from 1 through 100MB.            |
| <b>File Path</b>               | The path of the file where the appender logs the information.                                                                                                 |
| <b>Max Retention File Size</b> | The maximum retention file size for the log file.<br>The file size unit can be in KB or MB.<br>The value for the file size must be from 1 through 100MB.      |
| <b>Max Retention Time</b>      | The maximum retention time for the log file.<br>The value for the retention time must be from 1 through 180 days.                                             |

| Button        | Description                                                        |
|---------------|--------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                 |
| <b>Cancel</b> | Closes Edit Appender page and returns you to the Edit Logger page. |

### Attach Appender field descriptions

Use this page to assign an appender to the logger.

| Name                   | Description                                              |
|------------------------|----------------------------------------------------------|
| <b>Logger</b>          | The name of the logger.                                  |
| <b>Log Level</b>       | The level for which the logger logs the information.     |
| <b>Select Appender</b> | The list of appenders that you can assign to the logger. |

| Button        | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <b>Commit</b> | Assigns the appender to the logger.                                                  |
| <b>Cancel</b> | Closes the <b>Attach Appender</b> page and returns you back to the Edit Logger page. |



---

## Managing log viewer

### Log Viewer

Log Viewer displays all the logs generated by System Manager and the applications. The Log List displays a list of all the logs. You can view the details of each log, perform a search for logs, and filter specific logs. Log details include information about the event that generated the log, the severity level of the log, and other relevant information. You can search for logs based on search conditions and set filters to view logs that match the filter criteria. Log viewer displays logs that are of type Audit.

### Viewing log details

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Viewer**.
3. On the Logging page, select a log.
4. Click **View**.

### Exporting logs

You can export logs to a Comma Separated Values (.csv) file. You can open the CSV file using a text editor such as Wordpad, or a spreadsheet application such as Microsoft Excel.

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Viewer**.
3. On the Logging page, perform one of the following actions:
  - To export a log to a CSV file, select a log from the list and click **More Actions > Export Selected**.
  - To export the filtered logs to a CSV file, click **More Actions > Export All**.

When you use **Advanced Search** or **Filter** option to filter logs based on specific criteria, **Export All** exports all the filtered data

4. Click **Save** to save the exported log file to the local disk.

### Filtering logs

You can filter and view logs that meet the specified filter criteria. To apply the filters, you need to specify the filter criteria in the fields provided under select columns in the table displaying the logs. The column titles are the filter criteria. You can filter logs on multiple filter criteria.

## Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Viewer**.
3. On the Logging page, click **Filter: Enable** at the top right corner of the log table.
4. Enter or select the filter criteria.
5. Click **Filter: Apply**.

The page displays the logs that match the specified filter criteria.

### **Note:**

If no records matching the filter criteria are found, the Management Console application displays a message that no records matching the search criteria are found.

## Searching for logs

You can specify conditions for finding logs. The system displays logs that satisfy the search conditions. You can specify multiple search conditions.

## Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Log Viewer**.
3. On the Logging page, click **Advanced Search**.
4. In the **Criteria** section, from the first and second drop down fields, select the search criterion and the operator.
5. Select or enter the search value in the third field.
6. To add another search condition, click **+** and repeat steps 4 through 6.

Click **-** to delete a search condition. You can delete a search condition if you have more than one.

7. Select the **AND** or **OR** operator from the drop down field.

This page displays this drop down field when you specify more than one search condition.

8. Click **Search** to find the logs for the given search conditions.

## Logging field descriptions

The Logging page has two sections: the upper section contains buttons that allow you to view the selected log details, search for logs, and set filters. The lower section displays logs in a table. The table provides information about the logs. You can click the column title to sort the column data in ascending or descending order.

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b> | The option to select a log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Log ID</b>           | The unique identification number that identifies the log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Time Stamp</b>       | The date and time of the log generation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Host Name</b>        | The name of the system from which the log is generated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Product Type</b>     | The code that uniquely identifies the component which generated the log. For example, product, device, application, and service. An example of the log product type is GW600, which is a product type code identifier.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Severity</b>         | <p>The severity level of the log. The following are the type of severities:</p> <ul style="list-style-type: none"> <li>• <b>Emergency:</b> The system is unusable.</li> <li>• <b>Alert:</b> Action must be taken immediately.</li> <li>• <b>Critical:</b> Critical conditions.</li> <li>• <b>Error:</b> Error conditions.</li> <li>• <b>Warning:</b> Warning conditions.</li> <li>• <b>Notice:</b> Normal but significant condition.</li> <li>• <b>Informational:</b> Informational messages.</li> <li>• <b>Debug:</b> Debug-level messages.</li> </ul> <p> <b>Note:</b></p> <p>The colors of severities do not indicate logging severities.</p> |
| <b>Event ID</b>         | The unique identification number assigned to the event that generated the log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Message</b>          | A brief description of the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Process Name</b>     | The process on the device generating the message, usually the process name and process ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Facility</b>         | <p>The operating system, processes, and applications quantify messages into one of several categories. These categories generally consist of the generating facility, along with the severity of the message. The following are the types of supported facilities:</p> <ul style="list-style-type: none"> <li>• User-Level Messages</li> <li>• Security/authorization</li> <li>• Log Audit</li> </ul>                                                                                                                                                                                                                                                                                                                             |
| Button                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>View</b>             | Displays the Log - View Log Detail page. Use this page to view the details of the selected log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table continues...

| Button                                   | Description                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto-Refresh Mode</b>                 | Switches to the Auto-Refresh mode. When the Logging page is set in this mode, it automatically updates the logs in the table. This is a toggle button.                                                                                                                                                                                                         |
| <b>More Actions &gt; Export Selected</b> | Exports the selected logs to a CSV file. You can view the logs using Wordpad or Excel.                                                                                                                                                                                                                                                                         |
| <b>More Actions &gt; Export All</b>      | Exports all the logs to a CSV file. You can view the logs using the Wordpad or Excel application.<br><br> <b>Note:</b><br>When you use <b>Advanced Search</b> or <b>Filter</b> option to filter logs based on some criteria, <b>Export All</b> exports all the filtered data. |
| <b>Advanced Search</b>                   | The fields that you can use to specify the criteria for searching a log.                                                                                                                                                                                                                                                                                       |
| <b>Refresh</b>                           | Refreshes the log information in the table.                                                                                                                                                                                                                                                                                                                    |
| <b>Filter: Enable</b>                    | The fields under select columns that you can use to set filter criteria. This is a toggle button.                                                                                                                                                                                                                                                              |
| <b>Filter: Disable</b>                   | Hides the column filter fields without resetting the filter criteria. This is a toggle button.                                                                                                                                                                                                                                                                 |
| <b>Filter: Clear</b>                     | Clears the filter criteria.                                                                                                                                                                                                                                                                                                                                    |
| <b>Filter: Apply</b>                     | Filters logs based on the filter criteria.                                                                                                                                                                                                                                                                                                                     |
| <b>Select: All</b>                       | Selects all the logs in the table.                                                                                                                                                                                                                                                                                                                             |
| <b>Select: None</b>                      | Clears the selections.                                                                                                                                                                                                                                                                                                                                         |
| <b>Previous</b>                          | Displays the logs on the previous page. This button is not available if you are on the first page.                                                                                                                                                                                                                                                             |
| <b>Next</b>                              | Displays the logs on the next page. This button is not available if you are on the last page.                                                                                                                                                                                                                                                                  |

### Criteria section

This section appears when you click **Advanced Search** on the top right corner.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>Use this section to specify search conditions. Select the search criteria from the first drop down field. Select the operator from the second drop down list. Enter the search value in the text field.</p> <p>Select the following search criteria from the first drop down list:</p> <ul style="list-style-type: none"> <li>• Log ID: The unique identification number assigned to the log.</li> <li>• Host Name: Name of the system for which log is generated.</li> <li>• Product type: A code which uniquely identifies the component which generated the log. For example, product, device, application, and service.</li> <li>• Severity: Severity level of the log.</li> <li>• Message: Brief description of the log.</li> <li>• Event ID: Unique identification number assigned to the event.</li> <li>• Process Name: Process on the device generating the message.</li> <li>• Time Stamp: Date and time of the log generation.</li> <li>• Facility: The operating systems, processes, and applications quantify messages into one of several categories. These categories consist of the generating facility with the severity of the message.</li> </ul> <p>The second drop down list displays operators. Based on the search criteria that you select in the first drop down field, those applicable for the selected criteria are displayed in the second drop down list. The following are the list of operators:</p> <ul style="list-style-type: none"> <li>• Equals</li> <li>• Not Equals</li> <li>• Starts With</li> <li>• Ends With</li> <li>• Contains</li> </ul> <p>The operators for Time Stamp are: =, &gt;, &lt;, &gt;=, &lt;=, and !=.</p> <p>When you select Time Stamp from the first drop-down list, the page provides date and time fields for entering the date and time in the respective fields. Enter the date in MM/DD/YYYY format. You can select the date from the Calendar. You need to enter the time in one of the following formats:</p> <ul style="list-style-type: none"> <li>• 24Hr</li> <li>• AM</li> <li>• PM</li> </ul> |

| Button                       | Description                                                                        |
|------------------------------|------------------------------------------------------------------------------------|
| <b>Clear</b>                 | Clears the search criterion and sets the criterion to the default search criteria. |
| <b>Search</b>                | Searches the logs based on the search conditions.                                  |
| <b>Close/Advanced Search</b> | Hides the search fields.                                                           |
| <b>+</b>                     | Adds a search condition.                                                           |
| <b>-</b>                     | Deletes a search condition.                                                        |

## Logging field descriptions

Use this page to view logs in the Auto-Refresh mode. In this mode, the page updates the log information automatically.

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log ID</b>       | The unique identification number that identifies the log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Time Stamp</b>   | The date and time of the log generation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Host Name</b>    | The name of the system from which the log is generated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Product Type</b> | The code that uniquely identifies the component generating the log. For example, product, device, application, and service. GW600, which is a product type code identifier, is an example of the log product type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Severity</b>     | <p>The severity level of the log. The following are the type of severities:</p> <ul style="list-style-type: none"> <li>• <b>Emergency:</b> The system is unusable</li> <li>• <b>Alert:</b> Action must be taken immediately</li> <li>• <b>Critical:</b> Critical conditions</li> <li>• <b>Error:</b> Error conditions</li> <li>• <b>Warning:</b> Warning conditions</li> <li>• <b>Notice:</b> Normal but significant condition</li> <li>• <b>Informational:</b> Informational messages</li> <li>• <b>Debug:</b> Debug-level messages</li> </ul> <p> <b>Note:</b></p> <p>The colors do not indicate logging severities.</p> |
| <b>Event ID</b>     | The unique identification number assigned to the event generating the log.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Message</b>      | Brief description of the log. The message is generated based on the severity level of the log. For a log with severity level debug, the message contains information about debugging an error.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Process Name</b> | The process on the device that has generated the message. This is usually the process name and process ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

*Table continues...*

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Facility</b> | The operating system, processes, and applications quantify messages into one of several categories. These categories consist of the generating facility with the severity of the message. The following are the types of supported facilities: <ul style="list-style-type: none"> <li>• User-Level Messages</li> <li>• Security/authorization</li> <li>• Log Audit</li> </ul> |

| Button                      | Description                                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Logging Landing Page</b> | Switches the mode from Auto-Refresh to manual refresh and displays the Logging Home page. This is a toggle button. |

## Audit Logging

### Configuring audit logging

#### About this task

You can use the functionality to configure actions when the system encounters conditions such as:

- Audit failure
- 75% occupation of the audit partition
- 90% occupation of the audit partition

#### Procedure

1. On the System Manager web console, click **Services > Events**.
2. In the navigation pane, click **Logs > Audit Log Configuration**.
3. On the Audit Logging Configuration page, enter the relevant information in the fields.  
For more information, see “Audit Logging Configuration field descriptions”.
4. Click **Commit**.

### Audit Logging Configuration field descriptions

| Name                                               | Description                                                                                         |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Action on Audit Failure</b>                     | Field to select an action, which is performed after the audit failure.                              |
| <b>To Email Address on Audit Failure</b>           | Email address to which the notification is sent.                                                    |
| <b>Action on /var/log/audit partition 75% full</b> | Field to select an action, which is performed after 75% occupation of the audit-assigned partition. |

*Table continues...*

| Name                                                         | Description                                                                                              |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>To Email Address on /var/log/audit partition 75% full</b> | Email address to which the notification is sent.                                                         |
| <b>Action on /var/log/audit partition 90% full</b>           | Field to select an action, which is performed after 90% occupation of the audit-assigned partition.      |
| <b>To Email Address on /var/log/audit partition 90% full</b> | Email address to which the notification is sent.                                                         |
| <b>Email</b>                                                 | Option to send an email notification to the configured email address.                                    |
| <b>Trap</b>                                                  | Option to record an entry in the trap log file and send an email notification to the configured address. |
| <b>JBoss Server Shutdown</b>                                 | Option to shutdown the JBoss server and send a notification to the configured address.                   |

| Button        | Description                                                            |
|---------------|------------------------------------------------------------------------|
| <b>Commit</b> | Saves and commits any changes made in the audit logging configuration. |

---

## TrapListener service

The TrapListener service receives traps and informs from different applications and displays on the System Manager Alarming page.

- TrapListener receives V2c and V3 traps and informs defined in the common alarm definition file.
- TrapListener processes the Common Alarm Definition file for applications where all trap definitions are present.

You can configure the TrapListener service from **Services > Configurations** on the System Manager web console. For information on configuring the TrapListener service, see *Configuring the TrapListener service*.

If you change the Trap Listener settings as an administrator, you must create a new SNMP target profile for the System Manager IP address and a new SNMPv3 user profile for System Manager. The values in the new profiles must match the values in the Trap Listener settings. Attach the System Manager SNMPv3 user profile to the System Manager target profile, and attach the new SNMP target profile to all serviceability agents. For information on creating SNMP user profiles and target profiles and attaching the target profiles to serviceability agents, see *Managing Serviceability Agents* in *Administering Avaya Aura® System Manager*.

### Related links

[Configuring the TrapListener service](#) on page 889

[View Profile: TrapListener field descriptions](#) on page 889

[Serviceability Agents](#) on page 954



# Chapter 15: Managing licenses

---

## WebLM overview

Avaya provides a Web-based License Manager (WebLM) to manage licenses of one or more Avaya software products for your organization. WebLM facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com>.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server.

License activations in PLDS require the host ID of the WebLM server for inclusion in the license file. The host ID of the WebLM server is displayed on the Server Properties page of the WebLM server.

---

## Obtaining the license file

### About this task

For each licensed Avaya product that you are managing from the WebLM server, you can obtain a license file from PLDS, and install it on the corresponding WebLM server. For additional information on using PLDS, see *Getting Started with Avaya PLDS - Avaya Partners and Customers* at <https://plds.avaya.com>.

In Geographic Redundancy, you must generate the license file by using the host ID of primary System Manager.

### Caution:

Do not modify the license file that you receive from Avaya. WebLM does not accept a modified license file.

You require the host ID of the WebLM server to obtain the license file from PLDS. For client node locking, while generating the license file, you must provide the WebLM server host ID and client host ID.

### Procedure

1. Log on to the System Manager web console.
2. On the System Manager Web Console, click **Services > Licenses**.
3. In the left navigation pane, click **Server properties**.
4. Note the **Primary Host ID**.
5. Using the host ID, generate the license from PLDS.

### Related links

[Install license field descriptions](#) on page 1037

---

## Finding LAC for System Manager in PLDS

### About this task

You can find License Activation Code (LAC) using a Group ID or a SAP order number. With LAC, you can activate the available associated entitlements.

### Procedure

1. Log in to the PLDS at <https://plds.avaya.com>.
  2. From the Assets menu, select **View Entitlements**.
  3. In the **Application** field, select **System Manager**.
  4. Do one of the following:
    - To search using group ID, in the **Group ID** field, enter the appropriate group ID.
-  **Note:**
- All group IDs are numeric without any leading zeros.
  - To search using the SAP order number, click **Advanced Search**, and in the **Sales/Contract #** field, enter the SAP order number.
5. Click **Search Entitlements**

The system displays the LAC(s) in the search results.

---

## Accessing WebLM

### Before you begin

You require permissions to access the WebLM application.

## Procedure

1. Log on to the System Manager web console.
2. On the System Manager Web Console, click **Services > Licenses**.

---

## Installing a license file

### About this task

You can install a license file on the WebLM server. Use the Uninstall functionality to remove the license file from the WebLM server.

Licenses installed for WebLM Release 7.1 and later, must support SHA256 digital signature and 14-character host ID.

### Before you begin

- Get the license file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com>.
- Log on to the WebLM web console with administrator privilege credentials.
- For standard license file, remove the older license file before you install the new file.

#### **Note:**

The system displays an error message if an older license file is still available.

For centralized license file, the system automatically overwrites the older license file during installation.

For information about the license file installation errors while installing the license file, see *Administering standalone Avaya WebLM*.

## Procedure

1. In the navigation pane, click **Install license**.
2. On the Install license page, click **Browse**, and select the license file.
3. Read the terms and conditions, and click **Accept the License Terms & Conditions**.
4. Click **Install**.

WebLM displays a message on successful installation of the license file. The installation of the license file might fail for reasons, such as:

- The digital signature on the license file is invalid. If you get such an error, request PLDS to redeliver the license file.
- The current capacity use exceeds the capacity in the installed license.

### Related links

[Install license field descriptions](#) on page 1037

---

## Client node locking

WebLM supports client node locking of licenses where licenses are tied to specific application instances. You cannot move licenses across application instances. The feature is provided to support some Avaya data products that require licenses to be node-locked to an application instance or the client. For example, VPFM/COM. To use this feature, you must include the host IDs of the application instance and the WebLM server in the license file.

With the client node-locking feature:

- WebLM allows multiple licenses for a client node-locked product to be installed on the server at the same time. Each client node-locked license contains a unique host ID of the client.
- When a client node-locked license is installed on WebLM, WebLM automatically associates the license file with the client or application host ID that is included in the license file.
- The license request from the element would include the client/element host ID. WebLM serves licenses only if the client host ID in the request matches with any of the installed client node locked license files.
- WebLM enforces mutual TLS authentication for client node-locked licenses.
- The license over-install checks are based on the client host ID. While over-installing a license file with a new file for a client instance whose client host ID changed due to rehost, license file includes the old and new client host IDs. In this case, over-install check will be based on the old client host ID.

---

## Viewing the license capacity and utilization of the product features

### Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

### About this task

Use this procedure to view the license capacity and license utilization of a product for which you installed a license file.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View license capacity**.
  - If centralized licensing is disabled, the system displays the license capacity and the actual license usage of the product.
  - If centralized licensing is enabled, the system displays the **Installed License Files** table. Click the **Host ID - Centralized Licensing ID** hyperlink to view the license

capacity of the license file for the selected host ID. If the license file is assigned to an element then the system displays the element display name, centralized licensing ID, license owner, license host, and license file host IDs for the element.

#### Related links

[View License Capacity field descriptions](#) on page 1037

---

## Viewing peak usage for a licensed product

### Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the license file on the WebLM server for the licensed product.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View peak usage**.
  - If centralized licensing is disabled, the system displays the peak usage of the licensed features of the product.
  - If centralized licensing is enabled, the system displays the **Installed License Files** table. Click the **Host ID** hyperlink to view the peak usage of the license file for the selected host ID. If the license file is assigned to an element then the system displays the element display name and centralized licensing ID for the element.

#### Related links

[View Peak Usage field descriptions](#) on page 1038

---

## Uninstalling a license file

### Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Uninstall license**.
3. On the Uninstall license page, select the required license file.
4. Click **Uninstall**.

The system displays the Uninstall License Confirmation page.

5. Click **Uninstall** to confirm the license uninstallation.

If you do not have permission to uninstall the selected license file, the system only displays the **Cancel** button.

**Related links**

[Uninstall license field descriptions](#) on page 1044

---

## Viewing the server properties

**Before you begin**

Log on to the WebLM web console with administrator privilege credentials.

**Procedure**

In the left navigation pane, click **Server properties**.

**\* Note:**

The host ID specified in PLDS is embedded in the license file. You can install the license file only if the host ID of the server that hosts WebLM matches the host ID in the license file. Therefore, when you request for a license file, specify the correct host ID of the server that hosts WebLM.

**Related links**

[Server Properties field descriptions](#) on page 1045

---

## WebLM Home field descriptions

You can view information about the products and associated license files installed on the WebLM server.

| Name                        | Description                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Product Name</b>         | The name of the product for which the license file is installed.                                                                                                                                                             |
| <b>Product Version</b>      | The version of the product for which the license file is installed.                                                                                                                                                          |
| <b>Type of License</b>      | The type of license file installed for the product.<br>The options are: <ul style="list-style-type: none"><li>• <b>solution</b> (Avaya Subscription License)</li><li>• <b>standard</b></li><li>• <b>enterprise</b></li></ul> |
| <b>Date of Installation</b> | The date and time of installing the license file.                                                                                                                                                                            |
| <b>Active License Mode</b>  | The type of license file installed for the product.                                                                                                                                                                          |
| <b>License State</b>        | The status of the installed license file.                                                                                                                                                                                    |

*Table continues...*

| Name                                        | Description                                                |
|---------------------------------------------|------------------------------------------------------------|
| <b>Avaya Subscription License Available</b> | The availability status of the Avaya Subscription license. |
| <b>Standard License Available</b>           | The availability status of the standard license.           |

| Button                     | Description                                                                              |
|----------------------------|------------------------------------------------------------------------------------------|
| <b>Export All Licenses</b> | Exports the licenses to the <code>/tmp/all_licenses.zip</code> file on the WebLM server. |

---

## Install license field descriptions

| Name                                               | Description                                                                                            |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Enter license path</b>                          | The complete path where the license file is saved.                                                     |
| <b>Browse</b>                                      | The option to browse and select the license file.                                                      |
| <b>Avaya Global License Terms &amp; Conditions</b> | Avaya license terms and conditions that the user must agree to continue the license file installation. |

| Button         | Description                        |
|----------------|------------------------------------|
| <b>Install</b> | Installs the product license file. |

---

## View License Capacity field descriptions

| Name                         | Description                      |
|------------------------------|----------------------------------|
| <b>License File Host IDs</b> | The host ID of the license file. |

The following fields are applicable for the Solution license:

| Name                       | Description                                                                                                                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Active License Mode</b> | <p>The type of license active on WebLM.</p> <p>The default value is <b>Avaya Subscription</b>.</p> <p>The WebLM server can have Avaya Subscription and Standard (Perpetual) licenses installed. However, at a time only one license can be active. These licenses are used while switching between two modes.</p> |
| <b>License State</b>       | <p>The status of the Avaya Subscription license.</p> <p>The default value is <b>Granted</b>.</p>                                                                                                                                                                                                                  |

*Table continues...*

| Name                                        | Description                                                                                              |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Avaya Subscription License Available</b> | The availability status of the Avaya Subscription license on WebLM.<br>The default value is <b>Yes</b> . |
| <b>Standard License Available</b>           | The availability status of the standard license on WebLM.<br>The default value is <b>No</b> .            |

## Licensed Features

You can view the total number of feature licenses in the license file and the current usage of those licenses.

| Name                             | Description                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Feature (License Keyword)</b> | The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.                                  |
| <b>Expiration Date</b>           | The date on which the feature license expires.                                                                                                                                               |
| <b>Licensed capacity</b>         | The number of licenses for each licensed feature. WebLM fetches the number of feature licenses information from the license file.<br>For the Solution license, the value is <b>Metered</b> . |
| <b>Currently Used</b>            | The number of feature licenses that are currently in use by the licensed application. For features of type Uncounted, the column displays <i>Not counted</i> .                               |

## Acquired Licenses

The Acquired licenses table displays information about the licenses acquired by the licensed application. You can view the information in the table only if the licensed product has acquired feature licenses.

| Name               | Description                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------|
| <b>Feature</b>     | The feature keyword for each licensed feature that is currently acquired by a licensed application. |
| <b>Acquired by</b> | The name of the licensed application that has acquired the license.                                 |
| <b>Acquirer ID</b> | The unique identifier of the licensed application that has acquired the license.                    |
| <b>Count</b>       | The number of feature licenses that are currently acquired by the licensed application.             |

---

## View Peak Usage field descriptions

You can view information about the usage of feature licenses of a licensed application at different time intervals.



For the Solution license, the usage fields shows the number of used license file, but not the percentage (%) of usage.

| Name                                    | Description                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Feature (License Keyword)</b>        | The display name of the licensed features of the product and the keywords of each feature. The keywords represent the licensed feature in the license file.                                                                                                                                    |
| <b>Currently Allocated</b>              | The number of feature licenses purchased by the organization.<br>For the Solution license, the value is <b>Metered</b> .                                                                                                                                                                       |
| <b>Usage: qty/%</b>                     | The number of feature licenses for each licensed feature that a licensed application currently uses. The column also displays the percentage of usage.<br><br>For example, if 50 feature licenses are available and five feature licenses are used by applications, the column displays 5/10%. |
| <b>Peak Usage (today): qty</b>          | The highest number of feature licenses for each licensed feature used for the day.                                                                                                                                                                                                             |
| <b>Peak Usage (Last 7 days): qty/%</b>  | The highest number of feature licenses for each licensed feature used in the last seven days.<br><br>For example, if the peak usage for a feature license in the past seven days was 25, and the number of available licenses during these seven days was 50, then the column displays 25/50%. |
| <b>Peak Usage (Last 30 days): qty/%</b> | The highest number of feature licenses for each licensed feature used in the past 30 days.<br><br>For example, if the peak usage for a feature license in the past 30 days was 50, and the number of available licenses during these 30 days was 50, then the column displays 50/100%.         |
| <b>Time of Query</b>                    | The date and time when the last usage query for WebLM was executed.                                                                                                                                                                                                                            |
| <b>Status</b>                           | The success or failure of the last usage query executed for the WebLM server.                                                                                                                                                                                                                  |

| Button      | Description                                          |
|-------------|------------------------------------------------------|
| <b>Back</b> | Cancels the action and returns to the previous page. |

---

## Centralized licensing

---

### About centralized licensing

Some Avaya products do not share licenses from a single license file as each element instance requires a separate license file. You require a dedicated WebLM server to host the relevant license file of the associated element instance. In this licensing model, you require the same

number of WebLM servers as the number of products that you install and configure. In the virtualized environment, this model requires additional virtual machines for each element instance, thus increasing the VMware licensing cost. Thus, you cannot centrally manage the licenses for a product and must log in to each WebLM server and manage licenses for each element instance.

WebLM supports centralized licensing feature so that products can have multiple license files installed for multiple instances of the product. On a single WebLM server, you can install multiple license files of a product and associate specific license files to specific element instances.

After you enable centralized licensing from the WebLM interface, you can install multiple license files for the same product. You can add multiple element instances, and associate each license file to an element instance. The WebLM server provides licenses to the element instances based on the association you define.

---

## Enabling centralized licensing

### Before you begin

Install a product license file that supports centralized licensing. Centralized licenses contain the FEAT\_WLM\_CENTRALIZED feature in the product license file.

### About this task

By default, centralized licensing is disabled. You must enable centralized licensing to use this feature.

### Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Enable Centralized Licensing**.

#### **Warning:**

After enabling the Centralized Licensing feature for a product, you must link the license file to the associated product server instance. If you do not link the license file to a product server instance, the product server instance cannot acquire the license file from the WebLM server.

---

## Configure centralized licensing field descriptions

### Elements and License File Assignments

| Name                 | Description                                               |
|----------------------|-----------------------------------------------------------|
| Element Display Name | The display name that you enter for the element instance. |

*Table continues...*

| Name                                      | Description                                                                                                                                                                                                                                            |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Centralized Licensing ID</b>           | The element identifier for an element instance. The Centralized Licensing ID must match the name used by an element instance to acquire licenses from WebLM.<br><br>See the product documentation to find the name used by the element instance.       |
| <b>Host ID - Centralized Licensing ID</b> | The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product. |
| <b>License Host Name</b>                  | The host name of the license as defined in the license file.                                                                                                                                                                                           |
| <b>Date of Installation</b>               | The date of installation of the license file.                                                                                                                                                                                                          |

### Installed License Files

| Name                                      | Description                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Host ID - Centralized Licensing ID</b> | The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID. The centralized licensing ID is a unique number across multiple license files for the same product.                                                                       |
| <b>License Host Name</b>                  | The host name of the license as defined in the license file.                                                                                                                                                                                                                                                                 |
| <b>Assigned To Element</b>                | The field that indicates whether a license file is associated with an element instance. The possible values are: <ul style="list-style-type: none"> <li>• <b>Yes:</b> The license file is associated with an element instance.</li> <li>• <b>No:</b> The license file is not associated with an element instance.</li> </ul> |
| <b>Date of Installation</b>               | The date of installation of the license files.                                                                                                                                                                                                                                                                               |

| Button        | Description                                                               |
|---------------|---------------------------------------------------------------------------|
| <b>New</b>    | Adds an element instance and the mapping of an element to a license file. |
| <b>Edit</b>   | Edits the properties of the element instance.                             |
| <b>Delete</b> | Deletes an element instance.                                              |

## Adding an element instance and assigning the element instance to a license file

### Before you begin

Enable the Centralized Licensing feature.

Install the license files that you want to assign to an element instance.

## Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **New**.
4. On the Add Element Instance page, type the element display name, and the centralized licensing ID of the instance. For more information, see “Element instance field descriptions”.

The element ID must match the name used by an element instance to acquire licenses from WebLM. See the product documentation to find the name used by the element instance.

5. In the **Select License File** table, select the license file that you want to map to the element instance.
6. Click **Save**.

You can add an element instance and choose to map the license file later. In this scenario, you must type the element display name, the centralized licensing ID, and click **Save**.

## Related links

[Element instance field descriptions](#) on page 1043

---

# Editing an element instance and license file assignment

## Before you begin

- Enable the centralized licensing feature.
- Install the license file that you want to assign to the element instance.
- Add an element instance.

## Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. On the Configure Centralized Licensing page, select the element instance.
4. Click **Edit**.
5. On the Edit Element Instance page, modify the properties of the element instance. For more information see Element instance field descriptions
6. Click **Save**.

## Related links

[Element instance field descriptions](#) on page 1043

## Deleting an element instance

### Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. On the Configure Centralized Licensing page, select the element instance that you want to delete.
4. Click **Delete**.

The system displays the Delete Element Confirmation page.

5. Click **Delete**.

The system deletes the element instance and its assignment with the license file.

## Element instance field descriptions

| Name                            | Description                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Element Display Name</b>     | The display name that you enter for the element instance.                                                                                                                                                                                               |
| <b>Centralized Licensing ID</b> | <p>The element identifier for an element instance. The Centralized Licensing ID must match the name used by an element instance to acquire licenses from WebLM.</p> <p>See the product documentation to find the name used by the element instance.</p> |

### Select License File

| Name                                      | Description                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Host ID - Centralized Licensing ID</b> | <p>The host ID of the license file. The first 12 characters are the WebLM server host ID, and the last 5 characters are the centralized licensing ID.</p> <p>The centralized licensing ID is a unique number across multiple license files for the same product. For centralized licensing scenarios with just one license file, the host ID has 12 characters.</p> |
| <b>License Host Name</b>                  | The host name of the license as defined in the license file.                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assigned To Element</b>  | The field that indicates whether a license file is associated with an element instance. The possible values are: <ul style="list-style-type: none"> <li>• <b>Yes</b>: The license file is associated with an element instance.</li> <li>• <b>No</b>: The license file is not associated with an element instance.</li> <li>• <b>Yes</b>: The license file is associated with a Communication Manager server.</li> <li>• <b>No</b>: The license file is not associated with a Communication Manager server.</li> </ul> |
| <b>Date of Installation</b> | The date of installation of the license file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Button        | Description                                           |
|---------------|-------------------------------------------------------|
| <b>Save</b>   | Adds or edits the element instance.                   |
| <b>Cancel</b> | Cancels the add or delete element instance operation. |

## Disabling centralized licensing

### Before you begin

Ensure that:

- You have not added an element instance for the product. If you have added the element instances, delete the element instances.
- You have installed only a single license file for the product. If you have installed multiple license files, uninstall all the files except any one license file.

### Procedure

1. On the System Manager web console, click **Services > Licenses**.
2. In the navigation pane, click **Configure Centralized Licensing** for your licensed product.
3. Click **Disable Centralized Licensing**.

## Uninstall license field descriptions

Use this page to remove a license file from the WebLM server for a licensed product. The **Allocation Table License Files** table displays the ALF files. You cannot uninstall the ALF files.

| Name                     | Description                                             |
|--------------------------|---------------------------------------------------------|
| <b>License Host Name</b> | The WebLM server where the license files are installed. |
| <b>Host ID</b>           | The host ID of the license file.                        |

*Table continues...*

| Name                    | Description                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Products</b>         | The products for which licenses are installed on the WebLM server.                                                                   |
| <b>SID</b>              | The System ID of the license file.                                                                                                   |
| <b>Select Check box</b> | Use to select the license files that you require to remove from the WebLM server.<br><br>You cannot uninstall the ALF license files. |
| Button                  | Description                                                                                                                          |
| <b>Uninstall</b>        | Removes the selected license files from the WebLM server.                                                                            |

---

## Server Properties field descriptions

### Server Host ID

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Primary Host ID</b> | The MAC address of the server.<br><br>For non-VMware deployments, the primary host ID is the MAC address of the server.<br><br>For VMWare deployments, the primary host ID is a 14 character combination of the IP address and the UUID of the system.<br><br>You must use the host ID to generate licenses which you later install on the current instance of the WebLM server. |

---

## Adopter application cannot communicate with WebLM Server

### Cause

Due to higher security settings on the WebLM Server Release 7.1 system, the adopter applications that are using WebLM Server earlier to Release 7.1 might not communicate with WebLM Server to fetch the license file from WebLM Server by using the WebLM client.

### Solution

To fetch the license file from the WebLM Server Release 7.1 system, locate the `trusted_weblm_certs.jks` file from the adopter application system, take the backup of the file, delete the file, and then restart the adopter application.

Do this if the adopter application cannot communicate with WebLM Server regardless of the WebLM Server version on the adopter system.

---

# Enterprise licensing

---

## Configuring enterprise licensing

### Before you begin

- Log on to WebLM Home.
- Install the enterprise license file on the WebLM server for the product.

To verify the license file for a product, in the left navigation pane, click **Licensed products** and select the product. The content pane displays the product name, System Identification number (SID), and the license file type installed for the product at the top of the page.

### \* Note:

System Manager WebLM can be configured as master WebLM but cannot be configured as local WebLM to an external WebLM.

Standalone WebLM OVA-based deployment can be configured as master WebLM or local WebLM.

No other WebLM flavor can be configured as master WebLM.

|                                       | Enterprise Master WebLM | Enterprise Local WebLM |
|---------------------------------------|-------------------------|------------------------|
| System Manager WebLM                  | Yes                     | No                     |
| Standalone WebLM OVA-based deployment | Yes                     | Yes                    |
| Other WebLM flavors                   | No                      | Yes                    |

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. In the navigation pane, click **Enterprise configuration**.
3. On the Enterprise Configuration page, enter the appropriate information in the fields.

For more information, see “Enterprise Usage field descriptions”.

To successfully set up and configure the master WebLM server, enter valid information in the mandatory fields that are marked with a red asterisk.

4. In the **Master WebLM Configuration** section, enter the name, description, and IP address of the master WebLM server.
5. In the **Default Periodic Operation Settings** section, enter the retry count and the retry interval in minutes for the periodic operations.
6. In the **SMTP Server settings** section, enter the name of the SMTP server.
7. In the **E-mail notification settings for periodic operation** section, perform the following:
  - a. Set the **E-mail notification** to **On**.



- b. In the **E-mail address** field, enter an email address.
  - c. To add the email address to the list of recipients for the WebLM server to send email notifications, click **Add To List**.
8. In the **Default Periodic License Allocation Schedule** section, select the day and time for periodic license allocations.

The values you enter in this section remain as the default setting for periodic allocation for all local WebLM servers in the enterprise.

9. In the **Default Periodic Usage Query Schedule** section, select the day and time of the query for periodic usage.

The values you enter in this section remain as the default setting for periodic usage for all local WebLM servers in the enterprise.

 **Note:**

For any periodic operations, you must perform the manual allocation at least one time.

10. Click **Submit**.

The system validates the information. The system displays the host ID in the **Host ID** field. The host ID is the host ID of the computer where you installed the WebLM server.

#### Related links

[Enterprise Configuration field descriptions](#) on page 1055

[Enterprise Usage field descriptions](#) on page 1063

---

## Retrieving the local WebLM certificate from browser

### About this task

Use this procedure to retrieve the local WebLM certificate from the Firefox browser.

### Procedure

1. On the web browser, type the local WebLM server URL, `https://<Fully Qualified Domain Name>:<PortNumber>/WebLM`.
2. On the address bar, click the Lock icon.
3. Click the Show connection details icon.
4. Click **More Information**.
5. Click **View certificates**.
6. On the Certificate dialog box, do the following:
  - a. Click the **Details** tab.
  - b. Click **Export**.
  - c. Save the certificate to your local computer.

---

## Adding local WebLM certificate as trusted certificate in System Manager

### About this task

To add standalone WebLM as local WebLM in System Manager (master WebLM), you must add local WebLM certificate to the truststore of System Manager.

### Before you begin

Download the local WebLM certificate using the browser.

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select one or more element, and click **More Actions > Manage Trusted Certificates**.
3. On the Manage Elements page, select System Manager, and click **More Actions > Manage Trusted Certificates**.
4. On the Manage Trusted Certificates page, click **Add**.
5. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select the store type as **TM\_INBOUND\_TLS**.
6. Click **Import from file**.
7. Type the file name or click **Browse** to select a file.

 **Note:**

System Manager validates the file type. If you provide an invalid file type, the system displays an error message.

8. Click **Retrieve Certificate**.
9. Click **Commit**.
10. Restart the JBoss service on System Manager.

---

## Adding a local WebLM server

### Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Identify the WebLM servers that you must add as the local WebLM server.
- Configure the security certificate before you add a local WebLM server.
- On the Add Trusted Certificate page, select **Import using TLS**, and enter the appropriate information in the **IP Address** and the **Port** fields of the local WebLM server.

For more information, see Adding a Trusted Certificate in the Avaya Aura® System Manager help.

## Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Local WebLM Configuration > Add local WebLM**.
3. On the Local WebLM Configuration: Add local WebLM page, enter the appropriate information.  
  
To successfully set up and configure the local WebLM server, fields that are marked with a red asterisk (\*) are mandatory.  
  
For detailed descriptions of the fields, see “Add local WebLM field descriptions”.
4. In the **Local WebLM Configuration** section, enter the name, description, IP address, and port of the local WebLM server.
5. Select a protocol for the master WebLM server to communicate with the local WebLM server.
6. In the **Periodic license allocation schedule** section, select the day and time for periodic license allocations.
7. In the **Periodic usage query schedule** section, select the day and time of the query for periodic usage.
8. Click **Configure and validate**.

The system validates the information. If the information is valid, the system displays the host ID of the computer where the server is installed in the **Host ID** field.

## Related links

[Add local WebLM field descriptions](#) on page 1058

---

## Modifying a local WebLM server configuration

### Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Add at least one local WebLM server.

## Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Local WebLM Configuration > Modify local WebLM**.
3. On the Local WebLM Configuration: Modify local WebLM page, select the local WebLM server that you require to configure.
4. Click **Modify**.

The system displays another Local WebLM Configuration: Modify local WebLM page with a different set of WebLM configuration fields.

5. Modify the information in the following fields:

- In the **Local WebLM configuration** section, **Name**, **Description**, **Protocol**, and **Port**
- In the **Periodic License Allocation schedule** section, **Day** and **Time**
- In the **Periodic Usage Query schedule** section, **Day** and **Time**

6. Click **Modify**.

The system saves your changes.

#### Related links

[Modify local WebLM field descriptions](#) on page 1059

---

## Removing a local WebLM server

### Before you begin

- Log on to the WebLM web console with administrator privilege credentials.
- Install the enterprise license file.
- Add at least one local WebLM server.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Local WebLM Configuration > Delete local WebLM**.
3. On the Local WebLM Configuration: Delete local WebLM page, select the local WebLM server that you want to delete.
4. Click **Delete**.

 **Note:**

The system displays a warning message before removing the local WebLM server from the master WebLM server.

5. Click **OK**.

#### Related links

[Delete local WebLM field descriptions](#) on page 1061

---

## Viewing the license capacity of the licensed features of a product

### Before you begin

Log on to the WebLM web console with administrator privilege credentials.

## Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View by feature**.

## Related links

[View by feature field descriptions](#) on page 1055

---

# Viewing the connectivity status of the local WebLM servers

## Before you begin

Log on to the WebLM web console with administrator privilege credentials.

## Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **View by local WebLM**.

The page displays the connectivity status of the local WebLM servers.

## Related links

[View by local WebLM field descriptions](#) on page 1055

---

# Validating connectivity to local WebLM servers for a product

## Procedure

1. In the left navigation pane, click **Licensed products** and select the product name.
2. Click **Local WebLM Configuration**.
3. On the Local WebLM Configuration: View local WebLM page, select the local WebLM servers that you want to validate for connectivity.
4. To query the selected local WebLM servers, click **Validate Connectivity**.

## Result

The **status** column on the Local WebLM Configuration: View local WebLM page of the selected WebLM servers displays if the connection request made to the local WebLM server is successful.

## Related links

[View Local WebLMs field descriptions](#) on page 1057

---

# Viewing usage by WebLM

## Before you begin

Log on to the WebLM web console with administrator privilege credentials.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Usages > Usage by WebLM**.  
The system displays the Usages: Usage by WebLM page.
3. In the **Select WebLM** field, select the master or local WebLM server.
4. Click **Query System**.

### Related links

[Usage by WebLM field descriptions](#) on page 1062

---

## Viewing enterprise usage of a license feature

### Before you begin

Log on to the WebLM web console with administrator privilege credentials.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Usages > Enterprise Usage**.  
The system displays the Usages: Enterprise Usage page.
3. In the **Select Feature (License Keyword)** field, select the licensed feature.  
The page displays the usage of the licensed feature for the master WebLM server and the local WebLM servers.

### Related links

[Enterprise Usage field descriptions](#) on page 1063

---

## Viewing the periodic status of the master and local WebLM servers

### Before you begin

Log on to the WebLM web console with administrator privilege credentials.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Periodic status**.  
The system displays the Periodic Status page.

### Related links

[Periodic Status field descriptions](#) on page 1067

---

## Querying usage of feature licenses for master and local WebLM servers

### Before you begin

Log on to the WebLM web console with administrator privilege credentials.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Usages > Query Usage**.

The system displays the Usages: Query Usage page.

3. To view the usage details by feature licenses of a server, select the master or local WebLM server.
4. Click **Query Usage**.

If you select all WebLM servers or click **Check All** and click **Query usage**, the system displays the progress of the query request.

### Result

If you select one local WebLM server, the Usages: Usage by WebLM page displays the details of the local WebLM server you selected.

### Related links

[Query Usage field descriptions](#) on page 1064

---

## Changing allocations of licensed features for a local WebLM server

Use this functionality to change the license allocations of a feature that resides on a local WebLM server for the product.

### Procedure

1. Log in to the master WebLM server.
2. In the navigation pane, in **Licensed products**, click the required product.
3. Click **Allocations > Change allocations**.

The system displays the Allocations: Change Allocations page.

4. In the **New Allocation** column, enter the number of licenses you require to allocate for the feature that resides on a local WebLM server.
5. Click **Submit Allocations**.

## Related links

[Change Allocations field descriptions](#) on page 1066

---

## Viewing allocations by features

### Before you begin

Log on to the WebLM web console with administrator privilege credentials.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Allocations > View by feature**.

The system displays the Allocations: View by Feature page.

## Related links

[Allocations by Features field descriptions](#) on page 1065

---

## Viewing allocations by the local WebLM server

### Before you begin

Log on to the WebLM web console with administrator privilege credentials.

### Procedure

1. In the navigation pane, in **Licensed products**, click the required product.
2. Click **Allocations > View by local WebLM**.

The system displays the Allocations: View by Local WebLM page.

3. In the **Select Local WebLM** field, select the local WebLM server.

### Result

The page displays the allocation details for the local WebLM server you select.

## Related links

[Allocations by Local WebLM field descriptions](#) on page 1066

---

## Viewing usage summary

### Procedure

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, in **Licensed products**, click the required product.
3. Click **Usages**.



The system displays the Usage Summary page.

#### Related links

[Usage Summary field descriptions](#) on page 1061

## View by feature field descriptions

| Name                  | Description                      |
|-----------------------|----------------------------------|
| License File Host IDs | The host ID of the license file. |

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature (License Keyword) | The display name and the keyword for the licensed features of the product.                                                                                                                                                                                                                                                                                                                                 |
| License Capacity          | The total number of feature licenses that the organization purchases for each feature.                                                                                                                                                                                                                                                                                                                     |
| Currently available       | <p>The number of floating licenses of each feature that is currently available with the master WebLM server.</p> <p>The feature licenses that are not allocated to any local WebLM server are known as floating licenses.</p> <p> <b>Note:</b></p> <p>For uncouned features, this column displays <b>Not counted</b>.</p> |

## View by local WebLM field descriptions

Use this page to view the information related to local WebLM servers of a product.

| Name             | Description                                                                             |
|------------------|-----------------------------------------------------------------------------------------|
| Local WebLM name | Specifies the name of the local WebLM server.                                           |
| IP address       | Specifies the IP address of the local WebLM server.                                     |
| Last contacted   | Specifies the date and time when the local WebLM server was last contacted.             |
| Status           | Lists the success or failure of the last connection request to each local WebLM server. |

## Enterprise Configuration field descriptions

Use this page to specify the master WebLM server settings and the default settings for the periodic operations of the server. The settings you specify in the Enterprise Configuration Web page applies to the entire enterprise unless you override the setting while you add a local WebLM.

The master WebLM server uses the settings of the periodic operations to query itself and generate the usage report for licenses.

### Master WebLM Configuration

| Name               | Description                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | Specifies the name of the WebLM server.                                                                               |
| <b>Description</b> | Provides a brief description of the server.                                                                           |
| <b>IP address</b>  | Specifies the IP address of the WebLM server.                                                                         |
| <b>Host ID</b>     | Specifies the host ID of the computer where you installed the WebLM server. You cannot edit the <b>Host ID</b> field. |

### Default periodic operation settings

| Name                  | Description                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Retry count</b>    | Specifies the number of times a master WebLM server must try to connect to a local WebLM server for a periodic operation after a connection failure.<br><br>For example, set the count to 2. The master WebLM server makes an initial unsuccessful attempt to connect to a local WebLM server. The master WebLM server makes two more attempts to connect to the local WebLM server. |
| <b>Retry interval</b> | Specifies the duration in minutes, within which the retry count specified in the <b>Retry count</b> field must be carried out.<br><br>For example, suppose the <b>Retry count</b> is 2 and the Retry interval is 10 minutes. If the attempt to connect to the server fails, the master WebLM server makes two attempts in 10 minutes to connect to the local WebLM server.           |

### SMTP Server Settings

| Name               | Description                            |
|--------------------|----------------------------------------|
| <b>Server name</b> | Specifies the name of the SMTP server. |

### E-mail notification settings for periodic operation

| Name                       | Description                                                                                                                                                                                                                                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E-mail notification</b> | Specifies the e-mail notification. The notification options are: <ul style="list-style-type: none"> <li>• On: Sends an e-mail notification to the administrator if the periodic operations fail.</li> <li>• Off: Does not send an e-mail notification to the administrator if the periodic operations fail.</li> </ul> |

*Table continues...*

| Name                    | Description                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E-mail address</b>   | Specifies the e-mail address to which the WebLM application sends the e-mail notification if the periodic operations fail to execute.<br><br>* <b>Note:</b><br>Click <b>Add To List</b> to add the e-mail address in the list of recipients who must receive the e-mail notification of the periodic operation status. |
| <b>E-mail addresses</b> | Provides the list of e-mail addresses to which the WebLM application sends the e-mail notifications.                                                                                                                                                                                                                   |
| <b>Add To List</b>      | Adds the e-mail address that you enter in the <b>E-mail address</b> field to the list of recipients who must receive the e-mail notification of the periodic operation status.                                                                                                                                         |
| <b>Remove Selected</b>  | Removes the selected e-mail address from the <b>E-mail addresses</b> field.                                                                                                                                                                                                                                            |

### Default Periodic License Allocation Schedule

| Name        | Description                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Day</b>  | The day of the week on which the master WebLM server must send the ALF (Allocation license file) again to the local WebLM server. |
| <b>Time</b> | The time of the day specified in the <b>Day</b> field when master WebLM must send the ALF again to the local WebLM server.        |

### Default Periodic Usage Query Schedule

| Name        | Description                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Day</b>  | The day of the week on which the master WebLM server must query local WebLM servers for usage reports.                                 |
| <b>Time</b> | The time of the day you specify in the <b>Day</b> field when the master WebLM server must query local WebLM servers for usage reports. |

| Button        | Description                                                         |
|---------------|---------------------------------------------------------------------|
| <b>Submit</b> | Saves the enterprise configuration.                                 |
| <b>Reset</b>  | Resets the values in the fields to the values you previously saved. |

## View Local WebLMs field descriptions

Use this page to validate the local WebLM server connection. To validate the connection, the master WebLM server tries to connect to the specified local WebLM server.

\* **Note:**

To validate the connectivity of a local WebLM server, the local WebLM server must be already added for the product.

| Name                    | Description                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------|
| <b>Local WebLM Name</b> | The name of the local WebLM server.                                                     |
| <b>IP Address</b>       | IP address of the local WebLM server.                                                   |
| <b>Last Contacted</b>   | Date and time when the local WebLM server was last contacted.                           |
| <b>Status</b>           | Lists the success or failure of the last connection request to each local WebLM server. |

| Button                       | Description                                              |
|------------------------------|----------------------------------------------------------|
| <b>Validate Connectivity</b> | Validates the connectivity of the selected WebLM server. |
| <b>Check All</b>             | Selects all the local WebLM server.                      |
| <b>Clear All</b>             | Clears the selections of local WebLM servers.            |

## Add local WebLM field descriptions

### Local WebLM configuration

| Name               | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | The name of the server.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b> | A brief description of the server.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>IP Address</b>  | A unique IP address of the server. If you enter an IP address that is already configured for a local WebLM server, the system displays the message: <code>IP Address is being duplicated.</code>                                                                                                                                                                                                                                     |
| <b>Protocol</b>    | <p>The protocol scheme over which the master WebLM server communicates with the local WebLM server.</p> <p> <b>Note:</b></p> <p>If the local WebLM server that you add is a standalone WebLM server in Virtualized Environment, use HTTPS. You cannot use HTTP for communication with the standalone WebLM server in Virtualized Environment.</p> |
| <b>Port</b>        | The port number on which the master WebLM server communicates with the local WebLM server in the specified protocol scheme.                                                                                                                                                                                                                                                                                                          |
| <b>Host ID</b>     | The host ID of the computer on which you installed the server. You cannot edit the <b>Host ID</b> field.                                                                                                                                                                                                                                                                                                                             |

## Periodic License Allocation schedule

| Name        | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Day</b>  | <p>The day of the week on which the master WebLM server must send the ALFs again to the local WebLM server.</p> <p>By default, the system displays the settings specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.</p>                            |
| <b>Time</b> | <p>The time of the day specified in the <b>Day</b> field when the master WebLM server must send the ALFs again to the local WebLM server. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.</p> |

## Periodic Usage Query schedule

| Name        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Day</b>  | <p>The day of the week on which the master WebLM server must query local WebLM servers for usage reports. By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.</p>                                      |
| <b>Time</b> | <p>The time of the day specified in the <b>Day</b> field when the master WebLM server must query local WebLM servers for usage reports.</p> <p>By default, the system displays the settings you specified in the Enterprise Configuration. If you change the default settings, the new settings override the settings of the Enterprise Configuration. However, the change in the schedule is only applicable to this local WebLM server.</p> |

| Button                        | Description                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------|
| <b>Configure and validate</b> | Configures the local WebLM server and validates the creation of the local WebLM server. |
| <b>Back</b>                   | Returns to the View local WebLMs page.                                                  |

## Modify local WebLM field descriptions

Use this page to modify the information of a local WebLM server.

## Local WebLM configuration

| Name               | Description                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | Specifies the name of the server.                                                                                                                                                                                                                                                                                                          |
| <b>Description</b> | Displays a brief description of the server.                                                                                                                                                                                                                                                                                                |
| <b>IP Address</b>  | Specifies the IP address of the server.<br><br>* <b>Note:</b><br>You cannot modify the information in the <b>IP address</b> field.                                                                                                                                                                                                         |
| <b>Protocol</b>    | Specifies the protocol scheme over which the master WebLM server listens to the local WebLM server.<br><br>* <b>Note:</b><br>If the local WebLM server that you add is a standalone WebLM server in Virtualized Environment, use HTTPS. You cannot use HTTP for communication with the standalone WebLM server in Virtualized Environment. |
| <b>Port</b>        | Specifies the port number on which the master WebLM server listens to the local WebLM server in the specified protocol scheme.                                                                                                                                                                                                             |
| <b>Host ID</b>     | Specifies the host ID of the computer where you installed the server.<br><br>* <b>Note:</b><br>You cannot modify the information in the <b>Host ID</b> field.                                                                                                                                                                              |

## Periodic License Allocation schedule

| Name        | Description                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Day</b>  | Specifies the day of the week on which the master WebLM server must send the ALFs again to the local WebLM server.                                 |
| <b>Time</b> | Specifies the time of the day you entered in the <b>Day</b> field when the master WebLM server must send the ALFs again to the local WebLM server. |

## Periodic Usage Query schedule

| Name        | Description                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Day</b>  | Specifies the day of the week on which the master WebLM server must query the local WebLM servers for usage reports.                                 |
| <b>Time</b> | Specifies the time of the day you entered in the <b>Day</b> field when the master WebLM server must query the local WebLM servers for usage reports. |

| Button        | Description                                                                     |
|---------------|---------------------------------------------------------------------------------|
| <b>Modify</b> | Navigates to the Modify Local WebLM page for the local WebLM server you select. |

*Table continues...*

| Button      | Description                                                                    |
|-------------|--------------------------------------------------------------------------------|
| <b>Back</b> | Discards the configuration changes and returns to the Modify local WebLM page. |

---

## Delete local WebLM field descriptions

Use this page to delete a local WebLM server.

| Name                    | Description                                                       |
|-------------------------|-------------------------------------------------------------------|
| <b>Local WebLM name</b> | The name of the local WebLM server.                               |
| <b>IP address</b>       | The IP Address of the local WebLM server.                         |
| <b>check box</b>        | Use to select the local WebLM servers that you require to delete. |

| Button        | Description                                      |
|---------------|--------------------------------------------------|
| <b>Delete</b> | Removes the local WebLM server you selected.     |
| <b>Reset</b>  | Clears the selection of the local WebLM servers. |

---

## Deletion of the local WebLM server

Use the Delete Local WebLM option to delete the instance of a local WebLM server from the master WebLM server. When you delete a local WebLM server using the Delete Local WebLM option, the system does not remove the server physically. The master WebLM server sends a delete request to the local WebLM server. On receiving a delete request, the local WebLM server deletes the ALF of the product that is installed on the local WebLM server. The system deletes the instance of the local WebLM server from the master WebLM server, irrespective of the success or failure of the ALF deletion process on the local WebLM server.

If the master WebLM server is unable to send the delete request to the local WebLM server, the system deletes the instance of the local WebLM server from the master WebLM server. The ALF installed on the local WebLM server automatically expires after 30 days.

### Related links

[Delete local WebLM field descriptions](#) on page 1061

---

## Usage Summary field descriptions

Use this page to view the usage summary for a master WebLM server, a local WebLM server, or all the WebLM servers of the product.

| Name                 | Description                                                                                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WebLM Name</b>    | Displays the names of the master WebLM server and local WebLM servers of the product.                                                                                                                                                                                                                                  |
| <b>IP address</b>    | Specifies the IP address of the master WebLM server and local WebLM servers of the product.                                                                                                                                                                                                                            |
| <b>Time of Query</b> | Specifies the date and time when the system executed the last usage query for the WebLM server. If the status of the last usage query is <b>Failed</b> , this column also displays the date and time of the usage query that was last successful.                                                                      |
| <b>Status</b>        | Specifies the success or failure status of the last usage query that the system executed for each WebLM server. The <b>Status</b> column of a WebLM server remains blank if the server is not queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query. |

## Usage by WebLM field descriptions

Use this page to query the feature license usage by the master and local WebLM servers.

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select WebLM</b>                    | The master and local WebLM servers for which you can view the usage.                                                                                                                                                                                                                                                                       |
| <b>Feature (License Keyword)</b>       | The name and keyword of the counted features of the product.                                                                                                                                                                                                                                                                               |
| <b>Currently Allocated</b>             | The number of feature licenses for each feature that the system currently allocates to the selected WebLM server. For the master WebLM server of the product, this column lists the floating licenses available with the server.                                                                                                           |
| <b>Usage: qty/%</b>                    | The number of feature licenses for each feature that the licensed applications currently use from the allocated feature licenses. The column also displays the percentage of usage.<br><br>For example, if 50 feature licenses are allocated and applications use five feature licenses, this column displays 5/10%.                       |
| <b>Peak Usage (last 7 days): qty/%</b> | The highest number of feature licenses for each feature that the applications use in the past seven days. The column also displays the percentage of peak usage.<br><br>For example, if the peak usage in the past seven days was 25 and 50 feature licenses were available during the peak usage calculation, the column displays 25/50%. |

*Table continues...*



| Name                                        | Description                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Peak Usage (last 30 days):<br/>qty/%</b> | The highest number of feature licenses for each feature that the applications use in the past 30 days. The column also displays the percentage of peak usage.<br><br>For example, if the peak usage in the past 30 days was 50 and 50 feature licenses were available during the peak usage calculation, the column displays 50/100%. |
| <b>Time of Query</b>                        | The date and time when the system executed the usage query for the WebLM server you select.                                                                                                                                                                                                                                           |
| <b>Status</b>                               | The success or failure of the last usage query process executed for each WebLM server. The <b>Status</b> column remains blank if the server is queried even once for feature license usage. The usage query can be a periodic usage query or a nonperiodic usage query.                                                               |

| Button              | Description                                                      |
|---------------------|------------------------------------------------------------------|
| <b>Query System</b> | Queries the selected WebLM server for the feature license usage. |

## Enterprise Usage field descriptions

You can view the feature license usage of all WebLM servers for the selected feature.

| Name                                       | Description                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Feature (License Keyword)</b>    | Specifies the license features for which you can view the license usage.                                                                                                                                                                                                                                                                                      |
| <b>License capacity</b>                    | Specifies the total number of feature licenses the organization purchases for each feature.                                                                                                                                                                                                                                                                   |
| <b>Available</b>                           | Lists the number of licenses currently available with the master WebLM server.                                                                                                                                                                                                                                                                                |
| <b>WebLM Name</b>                          | Specifies the names of the WebLM servers of the product.                                                                                                                                                                                                                                                                                                      |
| <b>Currently Allocated</b>                 | Specifies the number of feature licenses that the system currently allocates to the WebLM servers for the selected feature.                                                                                                                                                                                                                                   |
| <b>Usage qty/%</b>                         | Specifies the number of feature licenses that the licensed applications currently use, from the allocated feature licenses for the selected feature. The column also displays the percentage of usage. For example, if 50 is the allocated feature licenses and 5 feature licenses have been used by the applications, this column displays 5/10%.            |
| <b>Peak Usage (last 7 days):<br/>qty/%</b> | Specifies the highest number of feature licenses that applications use in the past seven days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation is 50, the column displays 25/50%. |

*Table continues...*

| Name                                    | Description                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Peak Usage (last 30 days): qty/%</b> | Specifies the highest number of feature licenses that applications use in the past 30 days for the selected feature. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation is 50, the column displays 50/100%. |
| <b>Time of Query</b>                    | Specifies the date and time when the system executes the usage query for the selected feature.                                                                                                                                                                                                                                                           |
| <b>Status</b>                           | Specifies the status of the last usage query process that the system executes for each WebLM server. The status can be <i>Success</i> or <i>Failure</i> .                                                                                                                                                                                                |

## Query Usage field descriptions

Use this page to query the master WebLM server, a local WebLM server, or all the WebLM servers of the product for the feature license usage report.

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WebLM Name</b>       | <p>The names of the master and the local WebLM servers of the product as links. To view the feature license usage of a server, select the name of the required server in the <b>WebLM Name</b> column.</p> <p> <b>Note:</b></p> <p>If the specified WebLM server is not queried even once for feature license usage, the table on the Usage by WebLM page remains blank.</p>                                                                   |
| <b>IP address</b>       | The IP address of the master WebLM server and the local WebLM servers of the product.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Time of Query</b>    | <p>The date and time when the system executes the last usage query for the WebLM server. If the status of the last usage query is <i>Failed</i>, the <b>Time of Query</b> column displays the date and time of the usage query that was last successful.</p> <p> <b>Note:</b></p> <p>If the server does not receive a query request even once for feature license usage, the <b>Time of Query</b> column of a WebLM server remains blank.</p> |
| <b>Status</b>           | The success or failure of the last usage query that the system executes for each WebLM server. If the server does not receive a query request even once for feature license usage, the <b>Status</b> column of a WebLM server remains blank. The usage query can be a periodic usage query or a nonperiodic usage query.                                                                                                                                                                                                         |
| <b>Select Check box</b> | Use to select the WebLM server for which you require to determine the usage query.                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Button             | Description                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------|
| <b>Check All</b>   | Selects all the WebLM servers.                                                              |
| <b>Clear All</b>   | Clears the selections for all the WebLM servers.                                            |
| <b>Query Usage</b> | Queries the WebLM servers of the product you select for their feature license usage report. |

## Allocations by Features field descriptions

Use this page to view the feature license allocation information for each counted type feature of the product.

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Feature (License Keyword)</b> | Specifies the name and license keyword of the counted features of the product.                                                                                                                                                                                                                                                                                                              |
| <b>Local WebLM Name</b>          | Specifies the name of the local WebLM servers of the product. By default, this column is blank. The system displays the names of the local WebLM servers only when you select the arrow head in the <b>Feature (License Keyword)</b> column. If a local WebLM server does not exist for the product, the <b>Local WebLM Name</b> column remains blank for all the licensed features.        |
| <b>IP address</b>                | Specifies the IP addresses of the local WebLM servers of the product. By default, this column is blank. The system displays the IP address of the local WebLM servers only when you select the arrow-head in the <b>Feature (License Keyword)</b> column. If a local WebLM server does not exist for the product, the <b>IP address</b> column remains blank for all the licensed features. |
| <b>License Capacity</b>          | Specifies the total number of feature licenses purchased by the organization for the respective feature.                                                                                                                                                                                                                                                                                    |
| <b>Currently Allocated</b>       | Specifies the total number of feature licenses of the respective feature that the system allocated to the local WebLM servers of the product. If a licensed feature is not allocated to any local WebLM server, the system displays <code>zero</code> in the <b>Currently Allocated</b> column for the licensed feature.                                                                    |
| <b>Available</b>                 | Lists the number of floating licenses of the respective feature that is currently available with the master WebLM server.                                                                                                                                                                                                                                                                   |

### **Note:**

To view the information about the number of feature licenses of a feature that the system allocates to each local WebLM server, click the arrow-head beside the name of the required feature. The system displays new rows below the feature row with the feature license allocation information for each local WebLM server to which the feature is allocated.

## Allocations by Local WebLM field descriptions

You can view the feature license allocation information by local WebLM.

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Local WebLM</b>        | Specifies the local WebLM servers for which you can view the feature license allocation information.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Last Allocation</b>           | Specifies the date and time when feature licenses were last allocated to the local WebLM server you select.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Status</b>                    | Specifies the success or failure status of the last license allocation process that the system executes for the local WebLM server you select. The allocation process can be a periodic allocation process or a nonperiodic allocation process. If the status of the last license allocation process is <b>Failed</b> , and if the status of a previous license allocation process for the server is <b>Success</b> , the system displays the date and time of the last license allocation process that was successful in the <b>Last Allocation</b> field. |
| <b>Feature (License Keyword)</b> | Specifies the name and license keyword of the counted features that the system allocates to the local WebLM server.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>License Capacity</b>          | Specifies the total number of feature licenses the organization purchases for each feature.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Currently Allocated</b>       | Specifies the total number of feature licenses of each feature that the system allocates to the local WebLM server.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Available</b>                 | Lists the number of licenses currently available on the master WebLM server for allocation to local WebLM servers.                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Change Allocations field descriptions

Use this page to change current feature license allocation information for each local WebLM server of a product.

| Name                             | Description                                                                                                          |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Feature (License Keyword)</b> | The name and license keyword of the counted features that the system allocates to the local WebLM server you select. |
| <b>Local WebLM Name</b>          | The name of the local WebLM server.                                                                                  |
| <b>IP address</b>                | The IP addresses of the local WebLM servers of the product.                                                          |
| <b>License Capacity</b>          | The total number of feature licenses that the organization purchases for each feature.                               |
| <b>Currently Allocated</b>       | The total number of feature licenses of each feature that the system allocates to the local WebLM server you select. |

*Table continues...*

| Name                  | Description                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------|
| <b>Currently Used</b> | The total number of feature licenses of each feature that the product uses.                              |
| <b>Available</b>      | The number of floating licenses of each feature that is currently available with the local WebLM server. |
| <b>New Allocation</b> | The number of new licenses that the system allocates to a local WebLM server.                            |

| Button                    | Description                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Submit Allocations</b> | Allocates the number of feature licenses that you specify in the <b>New Allocation</b> field to the corresponding local WebLM servers. |
| <b>Reset</b>              | Resets the values that you specify in the <b>New Allocation</b> field to the previously saved value.                                   |

## Periodic Status field descriptions

Use the Periodic Status option to view the status of periodic operations such as the periodic allocation of the feature licenses to the local WebLM server and querying of the local WebLM server for usage report.

### Periodic Allocation

| Name                    | Description                                                                                                                                                                                                                                                                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Local WebLM Name</b> | Specifies the name of the local WebLM server of a product.                                                                                                                                                                                                                                                                                       |
| <b>IP Address</b>       | Specifies the IP addresses of all the local WebLM servers of the product.                                                                                                                                                                                                                                                                        |
| <b>Last Allocation</b>  | Displays the date and time when the system executed the last periodic license allocation process for each local WebLM server. If the status of the last periodic license allocation process is <b>Failed</b> , the <b>Last Allocation</b> column displays the date and time of the periodic license allocation process that was last successful. |
| <b>Status</b>           | Displays the success or failure status of the last periodic license allocation process that the system executed for each local WebLM server.                                                                                                                                                                                                     |

### Periodic Usage

| Name              | Description                                                                        |
|-------------------|------------------------------------------------------------------------------------|
| <b>WebLM Name</b> | Displays the name of the master WebLM server and local WebLM servers of a product. |
| <b>IP Address</b> | Displays the IP addresses of the master and local WebLM servers of a product.      |

*Table continues...*

| Name                    | Description                                                                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Usage Query</b> | Displays the date and time when the system executed the last periodic usage query for each WebLM server. If the status of the last periodic usage query is <code>Failed</code> , the <b>Last Usage Query</b> column also displays the date and time of the periodic usage query that was last successful. |
| <b>Status</b>           | Displays the success or failure status of the last periodic usage query that the system executed for each WebLM server. If the server is not queried even once for feature license usage, the <b>Status</b> column of a WebLM server remains blank.                                                       |

---

## Metering Collector configuration overview

With Release 8.1.2, you can manage the Avaya Subscription license on the WebLM server when metering collector is registered with WebLM. The metering collector configuration is applicable only for the Avaya Subscription license. The Solution-Avaya Subscription license contains more than one application.

Using the metering collector configuration, the WebLM server tracks the license usage information from the deployed applications. The WebLM server provides the license information to the metering collector when metering collector requests.

### Related links

[Metering Collector Configuration field descriptions](#) on page 1068

[Deleting the metering collector configuration](#) on page 1069

---

## Metering Collector Configuration field descriptions

If the metering collector is not registered with WebLM, the system displays the following message:

```
No Metering Collector currently configured for this WebLM.
```

```
Metering Collector is required for Avaya Subscriptions and is configured via the Metering Collector UI.
```

| Name        | Description                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b> | The name of the metering collector.<br><br>Each collector has its own unique metering collector id, which is displayed as <b>Name</b> on the WebLM server. |
| <b>URL</b>  | The URL of the metering collector. It contains the IP Address or FQDN of the metering collector.                                                           |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Link Status</b>           | <p>The status of the collector link. Default value of the status is <b>Active</b>.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Active</b></li> <li>• <b>Error</b></li> </ul> <p>WebLM checks the connectivity status in every 12 hours from the time last communication takes place with registered metering collector.</p> <p>If the metering collector does not send a request to WebLM for at least 24 hours, then the link status is displayed as <b>Error</b>.</p> |
| <b>Last Status Date/Time</b> | <p>The last synchronization timestamp of the metering collector with the WebLM server.</p> <p>The value is in the MM/DD/YYYY hh:mm:ss format.</p>                                                                                                                                                                                                                                                                                                                                                   |

| Button        | Description                                   |
|---------------|-----------------------------------------------|
| <b>Delete</b> | Deletes the metering collector configuration. |

**Related links**

[Metering Collector configuration overview](#) on page 1068

---

## Deleting the metering collector configuration

**Procedure**

1. Log on to the WebLM web console with administrator privilege credentials.
2. In the navigation pane, click **Metering Collector Configuration**.
3. On the Metering Collector Configuration page, click **Delete**.

The system displays the message: Are you sure you want to delete the collector configuration?

4. Click **Ok** to delete the metering collector configuration.

**Related links**

[Metering Collector configuration overview](#) on page 1068

# Chapter 16: Data Replication Service

---

## Data Replication Service

Data Replication Service (DRS) replicates data stored on the System Manager server to other element nodes or the slave nodes. DRS uses and extends SymmetricDS as the underlying mechanism for data replication.

SymmetricDS is an asynchronous data replication software that supports multiple subscribers and bi-directional synchronization. SymmetricDS uses Web and database technologies to replicate tables between relational databases in near real time. The system provides several filters while recording the data, extracting the data that has to be replicated to a slave node, and loading the data on the slave node.

Databases provide unique transaction IDs to rows that are committed as a single transaction. SymmetricDS stores the transaction ID along with the data that changed, so that it can play back the transaction at the destination node exactly the way it happened. This means that the target database maintains the same integrity as the source.

DRS provides a mechanism wherein elements can specify their data requirements in an XML document. On the basis of the XML document, DRS creates database triggers on the specified application tables and captures the database events for delivery to other element nodes. The client nodes then fetch these database events.

Data replication happens in two distinct phases:

- Full-sync. This is the initial replication phase, wherein whatever data the replica node requests is replicated to the client node.
- Regular-sync. This is the phase after full-sync, wherein subsequent change events are replicated to the replica node.

DRS supports the following modes of replication:

- Replication in Repair mode. In the repair mode, DRS replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of DRS.
- Automatic synchronization mode. After the database of the replica node is loaded with the requested data, the subsequent synchronizations of the master database and the replica database occur automatically. DRS replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after each fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. DRS creates replication batches whenever the data in the master database is added, modified, and deleted.



Using DRS, you can:

- View replica nodes in a replica group.
- Repair the replica nodes that are not synchronized. The repair action replicates the required data from System Manager.

---

## Synchronization in a Geographic Redundancy scenario

- DRS clients work with virtual IP or FQDN for a seamless switchover to the active System Manager when failover, failback, or split network occurs.
- DRS clients provide an audit mechanism to determine if the active System Manager contains the required data to resume synchronization. After a state change, the audit mechanism validates the last batch of data that is replicated to the element with the last batch of the data in the active System Manager. The state change includes failover, failback, and split network.
- During the audit, if the element contains more recent data than the data available on the active System Manager, the system marks the element for repair. Otherwise the system marks the element as in-sync with System Manager.

---

## DRS client audit

You can configure Data Replication Service (DRS) client elements in the Geographic Redundancy (GR) mode or GR-unaware mode.

A GR-aware DRS client must conform to the norms for a GR-aware element. A GR-aware element must work with the virtual FQDN configuration.

When you activate the secondary System Manager or when you enable GR after the system restores the primary System Manager, DRS marks all client nodes that are GR-aware for audit. The system displays the nodes marked for audit as *Pending Audit*. When you activate the secondary System Manager, DRS configures all GR-unaware DRS client nodes to deny recording any database change events. The system displays the state of DRS client nodes that are GR-unaware as *Not Managed*.

During the restoration of the primary System Manager, if you select the database of:

- The primary System Manager, the system marks all configured GR-aware client nodes for audit.
- The secondary System Manager, the system marks all DRS client nodes that are GR-aware for audit. Also, the system marks all DRS client nodes that are GR-unaware for repair.

When the system marks a node for audit, the system denies any further requests from the node until the audit is complete for that node. DRS service on System Manager sends a request to the DRS client element for audit data. DRS performs the audit for the DRS client and determines whether the client node requires a full synchronization. If the audit reveals that the client has more recent data than the data on System Manager, DRS schedules a full-synchronization for the

element. This phase marks the completion of audit and the system configures DRS to accept requests from the element.

Using DRS, the system initiates the client audit under following situations:

- **Manual:** When an administrator activates the secondary System Manager, DRS flags all configured clients for audit. This action ensures that none of the configured client elements have more data than the secondary System Manager. DRS flags similar client audit when the primary System Manager is recovered.
- **Automated:** During situations such as split network, when an administrator activates the secondary System Manager server, a node changes to the secondary System Manager server. However, in split network scenario, you cannot predict the network condition and the node can change back to the primary System Manager server.

---

## Viewing replica groups

### Procedure

On the System Manager web console, click **Services > Replication**.

### Result

The system displays the Replica Groups page with the groups in a table.

### Related links

[Replica Groups field descriptions](#) on page 1075

---

## Viewing replica nodes in a replica group

### About this task

You can view the replica nodes in a group.

### Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

Alternatively, you can click a replica group name displayed under the **Replica Group** column to view the replica nodes for that replica group.

The Replica Nodes page displays the replica nodes for the select group.

### Related links

[Replica Nodes field descriptions](#) on page 1076

---

## Repairing a replica node

### About this task

You can replicate data for a replica node whose database is not synchronized with the System Manager database. Repair is necessary if there is a post-install failure of Data Replication Service.

From Release 8.1, you can repair more than one replica nodes of a replica group.

### Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, perform one of the following:
  - Select a replica group, for which you want to repair the replica nodes, from the table displaying replica groups and click **View Replica Nodes**.
  - Click the name of the replica node under the **Replica Group** column.
3. On the Replica Nodes page, select one or more replica node, and click **Repair**.

The **Synchronization Status** column displays the data replication status for the selected replica node.

### Related links

[Replica Nodes field descriptions](#) on page 1076

---

## Repairing all replica nodes in a replica group

### About this task

You can replicate data for all the replica nodes that are in a group. You can perform this operation if replica nodes in a group are not synchronized with the System Manager database.

### Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, select a replica group for which you want repair the replica nodes from the table displaying replica groups.
3. Click **Repair**.

The **Synchronization Status** column displays the data replication status for the replica group.

---

## Viewing replication details for a replica node

You can view the batch-related information such as total number of batches received, processed, and skipped for a replica node. The master database sends the requested data in batches to the replica node.

### Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, select a replica group and click **View Replica Nodes**.

The Replica Nodes page displays the replica nodes for the selected replica group in a table.

3. Select a replica node and click **View Details**.

The Data Replication page displays the replication details for the selected replica node.

### Related links

[Replication Node Details field descriptions](#) on page 1079

---

## Removing a replica node

### About this task

From Release 8.1, you can remove more than one replica nodes from a replica group.

### Procedure

1. On the System Manager web console, click **Services > Replication**.
2. On the Replica Groups page, select the replica group from which you need to remove a node, and click **View Replica Nodes**.
3. On the Replica Node page, select one or more replica nodes, and click **Remove**.

---

## Removing a replica node from the queue

### About this task

From Release 8.1, you can remove more than one replica nodes from the queue of a replica group.

### Procedure

1. On the System Manager web console, click **Services > Replication**.

2. On the Replica Groups page, select the replica group for which you must remove the node, and click **View Replica Nodes**.
3. On the Replica Node page, select one or more replica node, and click **Remove from Queue**.

## Replica Groups field descriptions

The replica groups are logical groupings of the replica nodes. You can use the replica groups field descriptions page to:

- View all the replica groups in the enterprise.
- View the replication status of the replica groups.

The page displays the following fields when you select **All** from the **Replica Group** field.

| Name                          | Description                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select check box</b>       | An option to select a replica group.                                                                                                                                                  |
| <b>Replica Group</b>          | The name of the replica group. Each replica group in the list is a hyperlink. When you click a group, the system displays the replica nodes for that group on the Replica Nodes page. |
| <b>Synchronization Status</b> | For each replica group, displays the combined synchronization status of all replica nodes under the group                                                                             |
| <b>Group Description</b>      | A brief description of the replica group.                                                                                                                                             |

| Button                    | Description                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Replica Nodes</b> | Displays the Replica Nodes page. Use this page to view replica nodes for a group that you select.                                                                     |
| <b>Repair</b>             | Initiates full-sync for the selected groups and effectively for all the replica nodes that belong to the selected groups.                                             |
| <b>Filter: Enable</b>     | Displays fields under <b>Replica Group</b> and <b>Synchronization Status</b> columns where you can set the filter criteria. <b>Filter: Enable</b> is a toggle button. |
| <b>Filter: Disable</b>    | Hides the column filter fields without resetting the filter criteria. <b>Filter: Disable</b> is a toggle button.                                                      |
| <b>Filter: Apply</b>      | Filters replica nodes based on the filter criteria.                                                                                                                   |

---

## Replica Nodes field descriptions

You can use this page to:

- View the replica nodes in a selected replica group when you request data replication from the master database of System Manager.
- View the replication status of the replica nodes in a group.

| Name                   | Description                                                                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select check box       | Provides the option to select a replica node.                                                                                                                                                                    |
| Replica Node Host Name | Displays the full hostname of the replica node.<br><br>If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com. |
| Product                | Displays the name of the product.                                                                                                                                                                                |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Synchronization Status</b> | <p>Displays the synchronization status of the replica node.</p> <p>When you install a node, the node goes from a <b>Ready for Repair</b> state to the <b>Queued for Repair</b> to <b>Repairing</b>, and finally to the <b>Synchronized</b> state. During this phase, the replica node receives a full-sync, wherein configured data is replicated to the replica node. Once the replica node is prepared with a full-sync, thereafter the node receives the subsequent changes in the form of regular-sync.</p> <p>A replica node can be in any one of the following states during the lifecycle:</p> <ul style="list-style-type: none"> <li>• <b>Ready for Repair:</b> The database of the replica node is not synchronized with the master database.</li> <li>• <b>Queued for Repair:</b> The replication request of the replica server is in queue with other data replication requests. The color code of the status is yellow.</li> <li>• <b>Repairing:</b> The data replication process is in progress. The color code of the status is yellow.</li> <li>• <b>Synchronized:</b> The system has successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green.</li> </ul> <p> <b>Note:</b></p> <p>If you encounter the following, contact the administrator who can manually intervene to resolve the problem:</p> <ul style="list-style-type: none"> <li>• <b>Not Reachable:</b> System Manager is unable to connect to the replica node. This indicates that the replica node is switched off for maintenance, a network connectivity failure, or any other issue that affects general connectivity between System Manager and the replica node.</li> <li>• <b>Synchronization Failure:</b> Data replication is broken between System Manager and the replica node. This status generally indicates a catastrophic failure.</li> </ul> <p>During the automatic replication of data from the master to the replica node, the system displays the following status:</p> <ul style="list-style-type: none"> <li>• <b>Synchronizing:</b> The data replication is in progress for the replica node. The color code of the status is yellow.</li> <li>• <b>Synchronized:</b> The system successfully replicated the data that the replica node requested from the master database to the database of the replica node. The color code of the status is green.</li> <li>• <b>Pending Audit:</b> The replica node is marked for audit. In this state, DRS dishonors any request from the node until audit is successfully conducted for the node. On completion of audit activity, the node</li> </ul> |

*Table continues...*

| Name                                 | Description                                                                                                                                                                             |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      | displays any of the other states as applicable. The color code of the status is yellow.                                                                                                 |
| <b>Last Synchronization Time</b>     | Displays the last time when the system performed the data synchronization or replication for the replica node.                                                                          |
| <b>GR Capable</b>                    | Displays whether the replica node is GR-capable or not.                                                                                                                                 |
| <b>Last Replication Request Time</b> | Displays the time when a pre-7.0 replica node last requested System Manager for data or the time when System Manager last tried to send data to a replica node on Release 7.0 or later. |

| Button                         | Description                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>View Details</b>            | Displays the Data Replication page. Use this page to view the synchronization details for a replica node.      |
| <b>Repair</b>                  | Replicates or resynchronizes data from the master node to a selected replica node.                             |
| <b>Remove</b>                  | Removes the nodes you select from the replica group.                                                           |
| <b>Remove From Queue</b>       | Removes the replica node you select from the queue.                                                            |
| <b>Show All Replica Groups</b> | Returns to the Replica Groups page.                                                                            |
| <b>Advanced Search</b>         | The link to perform advance search. When you click on this link, System Manager displays the Criteria section. |
| <b>Filter: Enable</b>          | The fields where you can set the filter criteria. <b>Filter: Enable</b> is a toggle button.                    |
| <b>Filter: Disable</b>         | Hides the column filter fields. <b>Filter: Disable</b> is a toggle button.                                     |
| <b>Filter: Apply</b>           | Filters replica nodes based on the filter criteria.                                                            |
| <b>Select: All</b>             | Selects all replica nodes in the table.                                                                        |
| <b>Select: None</b>            | Clears the selection for the users that you select.                                                            |
| <b>Refresh</b>                 | Refreshes the replica node information in the table.                                                           |

## Criteria

| Name                          | Description                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Search Criteria</b> | <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>Replica node name</b></li> <li>• <b>Synchronization time</b></li> <li>• <b>Synchronization Status</b></li> </ul> |

*Table continues...*



| Name                          | Description                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Search Operator</b> | The options are: <ul style="list-style-type: none"> <li>• <b>Equals</b></li> <li>• <b>Not Equals</b></li> <li>• <b>Starts with</b></li> <li>• <b>Ends with</b></li> <li>• <b>Contains</b></li> </ul> |
| <b>Enter Search to Text</b>   | Specify the search criteria.                                                                                                                                                                         |

| Button        | Description                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| -             | Removes the additional search criteria fields.<br>This field is enabled when the additional search criteria fields are added. |
| +             | Adds the additional search criteria fields.                                                                                   |
| <b>Clear</b>  | Clears the search criteria.                                                                                                   |
| <b>Search</b> | Performs the search for the specified search criteria                                                                         |
| <b>Close</b>  | Closes the Criteria section.                                                                                                  |

## Replication Node Details field descriptions

You can use this page to view the following details:

- The batch-related information such as total number of batches received, processed, and skipped for a replica node.
- The last time when the replication server performed the synchronization or replication.
- Synchronization or replication error details.

### General

| Name                          | Description                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replica Node Group</b>     | Displays the name of the group that the replica node belongs to. A node-group is a logical grouping of similar nodes.                                                                                            |
| <b>Replica Node Host Name</b> | Displays the full hostname of the replica node.<br><br>If you need to administer Session Manager, the Replica Nodes Web page displays the fully qualified domain name. For example, ab-ct10-defg-bsm.mydata.com. |
| <b>Last Down Time</b>         | Displays the last time and date when the replica node could not be reached. System Manager periodically checks whether a replica node is reachable.                                                              |

*Table continues...*

| Name                          | Description                                                                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Repair Start Time</b> | Displays the last time and date when a full-sync was started for the node.                                                                                                              |
| <b>Last Repair End Time</b>   | Displays the last time and date when a full-sync was completed for the node.                                                                                                            |
| <b>Last Pull Time</b>         | Displays the time when a pre-7.0 replica node last requested System Manager for data or the time when System Manager last tried to send data to a replica node on Release 7.0 or later. |
| <b>Build Version</b>          | Displays the version of the element configuration.                                                                                                                                      |
| <b>GR Capable</b>             | Displays whether the replica node is GR-capable or not.                                                                                                                                 |

### Synchronization Statistics

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pending Batches</b>           | Lists the batches that are yet to be replicated to the replica node.<br><br>During the data replication process, System Manager records the changes for a particular replica node in the form of events. When a replica node requests System Manager for change events, the change events are made into batches. These batches are then replicated to the replica node. |
| <b>Pending Unbatched Events</b>  | Lists the change events that are yet to be formed into batches.<br><br>The recorded change events are formed into batches and only a predefined number of batches are replicated to a replica node in a request. The remaining events wait for the subsequent request from the replica and are called unbatched events pending batching and subsequent replication.     |
| <b>Synchronization Status</b>    | Displays the synchronization status of the replica node. For details, see Replica Nodes field descriptions.                                                                                                                                                                                                                                                             |
| <b>Last Synchronization Time</b> | Displays the last time when the system performed the data synchronization or replication for the replica node.                                                                                                                                                                                                                                                          |
| <b>Last Batch Acknowledged</b>   | Displays the last batch that an element acknowledged as successfully processed on the element side.<br><br>During an audit, Data Replication Service (DRS) compares the last successfully committed batch on the node with the data in the last batch acknowledged batch. If the node has a more recent batch, then DRS schedules a full-sync for the node.             |

*Table continues...*

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Marked For Audit</b> | <p>Marks all replica nodes that are GR-enabled for audit:</p> <p>The status can be:</p> <ul style="list-style-type: none"> <li>• : Indicates that the node is marked for audit.</li> <li>• : Indicates that the node is not marked for audit.</li> </ul> <p>When the node is marked for audit, the replica status changes to <b>Pending Audit</b>, and the color changes to yellow.</p> <ul style="list-style-type: none"> <li>• When you activate the secondary System Manager or when you enable GR after the primary System Manager restores</li> <li>• When the primary System Manager restores and you choose the database of the primary System Manager</li> <li>• When the primary System Manager restores and you choose the database of the secondary System Manager</li> </ul> <p>DRS denies any request from the replica node that is marked for audit until the audit is complete for the replica node.</p> |
| <b>Last Audit Time</b>  | Displays the last time and date when DRS performed the audit of data from the node that is marked for audit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

### Last Error Details

| Name                  | Description                                                       |
|-----------------------|-------------------------------------------------------------------|
| <b>Cause of Error</b> | Describes why the system failed to replicate or synchronize data. |
| <b>Time of Error</b>  | Displays the time when the error occurred.                        |

| Button         | Description                             |
|----------------|-----------------------------------------|
| <b>Refresh</b> | Refreshes the Replication Node details. |
| <b>Done</b>    | Returns to the Replica Nodes page.      |

# Chapter 17: Managing reports

---

## Reports

Avaya Aura® System Manager supports the Reports feature for communication objects. System Manager has about 350 predefined List and Display Communication Manager configuration reports.

You can use this feature to:

- Generate Communication Manager object reports in various formats, such as CSV, PDF, HTML, and Other (.txt with delimiter).
- Create and manage reports.
- Edit report parameters.
- Rerun reports.
- Customize the report contents.
- Save reports in the System Manager server.
- View and delete reports stored in System Manager.
- Save reports to a local computer.
- Email reports to one or more addresses. You can configure an email server to send reports.

You can assign permissions for reports and generate reports for the specific custom user.

---

## Support for generating endpoint reports with buttons

With System Manager Release 7.1.3.2 and later, you can generate an endpoint report for the following:

- **Main Buttons**
- **Feature Buttons**
- **Expansion/Module Button**
- **SoftKeys Buttons**

For generating an endpoint report with a button, you must generate:

- The report in the CSV format.
- The Detailed (Database) report.

For information about how to generate the Detailed report, see “Generating a detailed report”.

## Reports Generation field descriptions

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Used Space</b> | The maximum space allocated for storing the generated reports. If the report files exceed the maximum file size of 1 GB, the system generates an alarm. You must manually delete some files before you can generate a new report.<br><br>On the <b>Services &gt; Configurations &gt; Settings &gt; Reports &gt; Configuration</b> page, you can configure <b>Reports Output Directory Properties</b> . For more information, see View Profile:Configuration field descriptions. |

### Reports Definition List

| Name                 | Description                                                             |
|----------------------|-------------------------------------------------------------------------|
| <b>Name</b>          | The name of the report.                                                 |
| <b>Host Name(s)</b>  | The Communication Manager instance from which the report was generated. |
| <b>Creation Date</b> | The date when the report was generated.                                 |
| <b>Created By</b>    | The user who created the report.                                        |
| <b>Format</b>        | The format in which the report was generated.                           |
| <b>Object</b>        | The Communication Manager object used for generating the report.        |

| Button                 | Description                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------|
| <b>Edit</b>            | Displays the Edit Report Definition page to edit the selected report.                          |
| <b>New</b>             | Displays the New Report page to create a new report.                                           |
| <b>Run Now</b>         | Runs the selected report immediately.                                                          |
| <b>Delete</b>          | Deletes the selected report.                                                                   |
| <b>Filter: Enable</b>  | Displays fields where you can set the filter criteria. This is a toggle button.                |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button. |
| <b>Filter: Clear</b>   | Clears the filter criteria.                                                                    |
| <b>Filter: Apply</b>   | Filters reports based on the criteria.                                                         |

## Related links

[View Profile:Configuration field descriptions](#) on page 869

---

# Generating a detailed report

## Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Generation**.
3. On the Reports Definition List page, click **New**.
4. On the New Report page, in the **Application** field, click **Communication Manager**.
5. In the Communication Manager table, select one or more Communication Manager instances.
6. Click **Next**.
7. Select **Detailed (Database)** to generate the report for Communication Manager objects in the database.
8. Select the report type from **Report Type**.
9. On the Reports Generation page, in **Available Fields**, select the fields to include in your report.
10. Click the right arrow icon.   
The **Selected Field** table displays the selected fields. By default, some fields are already available in the **Selected Fields** column.
11. Click **Next**.
12. On the Report Parameters page, complete the report parameters, and click **Generate Report**.  
You can only generate a **Detailed (Database)** report if the Initializing synchronization for the specific Communication Manager instances is successful. Otherwise, report generation fails.
13. To download and view the report, go to **Services > Reports > History**.

## Related links

[New Report field descriptions](#) on page 1085

# Generating a basic report

## Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Generation**.
3. On the Reports Definition List page, click **New**.
4. On the New Report page, in the **Application** field, select **Communication Manager**.
5. From the Communication Manager table, select one or more Communication Manager instances.
6. Click **Next**.
7. Click **Basic (List and Display)** to generate a report directly from Communication Manager.
8. On the Basic Report page, select **Report Type**.

You can generate a **List** report or a **Display** report.

9. In the **Communication Manager Object** field, select Communication Manager object to generate a report.
  10. In the **Qualifier** field, type the qualifier for the Communication Manager object.
  11. Click **Next**.
  12. On the Report Parameters page, complete the report parameters, and click **Generate Report**.
- You can only generate a **Basic** report if the Initializing synchronization for the specific Communication Manager instances is successful. Otherwise, report generation fails.
13. To download and view the report, go to **Services > Reports > History**.

## Related links

[New Report field descriptions](#) on page 1085

# New Report field descriptions

## New Report

| Name               | Description                                                                 |
|--------------------|-----------------------------------------------------------------------------|
| <b>Application</b> | The application type for which you want to generate the report.             |
| <b>Name</b>        | The name of the element instance that you choose for generating the report. |
| <b>Host</b>        | The Communication Manager system that you select for generating the report. |

**Basic (List and Display)**

| Name                                | Description                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Report Type</b>                  | The report type. You can generate a <b>List</b> report or a <b>Display</b> report for the Communication Manager object you select. |
| <b>Communication Manager Object</b> | The Communication Manager object that you select for generating the report.                                                        |
| <b>Name</b>                         | The name of the element instance that you choose for generating the report.                                                        |
| <b>Host</b>                         | The Communication Manager system that you select for generating the report.                                                        |
| <b>Qualifier</b>                    | The qualifier for the Communication Manager object that you select for generating the report.                                      |

**Detailed (Database)**

| Name                    | Description                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Report Type</b>      | The Communication Manager object that you choose for generating the report.                                                                 |
| <b>Available Fields</b> | The fields that you want to generate as part of the report. The fields vary according to the Communication Manager object you choose.       |
| <b>Selected Fields</b>  | The fields that you select from <b>Available Fields</b> . The report that you generate displays only the fields in <b>Selected Fields</b> . |

| Button                                | Description                                                                                                    |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Move selected columns to right</b> | Moves selected fields to the right in the <b>Selected Fields</b> column.                                       |
| <b>Move selected columns to left</b>  | Moves selected fields to the left in the <b>Available Fields</b> column.                                       |
| <b>Move all columns to right</b>      | Moves all the fields to the right in the <b>Selected Fields</b> column.                                        |
| <b>Move all columns to left</b>       | Moves all the fields to the left in the <b>Available Fields</b> column.                                        |
| <b>Reset to default columns</b>       | Resets your selection. The system displays the default fields when you click <b>Reset to default columns</b> . |
| <b>Move Up</b>                        | Moves up the selected field by one position in the <b>Selected Fields</b> column.                              |
| <b>Move Down</b>                      | Moves down the selected field by one position in the <b>Selected Fields</b> column.                            |

**Report Parameters**

| Name               | Description                                                                         |
|--------------------|-------------------------------------------------------------------------------------|
| <b>Report Name</b> | The name of the report. Type a name of your choice in the <b>Report Name</b> field. |

*Table continues...*



| Name                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select file format</b>          | The format in which you want to generate the report. The options are: <ul style="list-style-type: none"> <li>• <b>CSV</b></li> <li>• <b>PDF</b></li> <li>• <b>HTML</b></li> <li>• <b>Other (.txt with delimiter)</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Select delimiter</b>            | The delimiter that you want to apply while generating the report. The options are: <ul style="list-style-type: none"> <li>• <b>comma</b></li> <li>• <b>semicolon</b></li> <li>• <b>space</b></li> <li>• <b>tab</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Append to existing report</b>   | The data appended to the existing report.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Append date to Report File</b>  | The date appended to the report file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Select destination location</b> | The location where you want to save the generated report. The options are: <ul style="list-style-type: none"> <li>• <b>Local</b> (Path : /swlibrary/reports_data): The option to save the generated report to your local computer. By default, the path is /swlibrary/reports_data.</li> <li>• <b>Remote Server</b>: The option to save the generated report to a <b>Remote server</b>. Do one of the following: <ul style="list-style-type: none"> <li>- Select the <b>Remote Server</b> from the drop-down field to store your reports.</li> <li>- Select the field where you want to store the reports: <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>IP</b></li> <li>• <b>Type</b></li> <li>• <b>Remote Server From</b></li> <li>• <b>Default Server</b></li> </ul> </li> </ul> </li> <li>• <b>Email</b>: The option to enter one or more email addresses you want to send the report. To enter multiple email addresses, separate them by a semicolon.</li> </ul> |

*Table continues...*

| Name                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Customize Report</b> | <p>The option to create a customized report. Click one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Customize Report Header:</b> The option to choose the title of your choice.</li> <li>• <b>Export Column Titles on First Row:</b> The option to export the column titles of your report.</li> </ul> <p>If you select this option, the first page displays only the column headers that you select. Other pages display the default report headers.</p> |
| <b>Schedule Job</b>     | <p>The scheduler options to schedule the report generation job. Click one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Now:</b> To generate the report immediately.</li> <li>• <b>Later:</b> To generate the report at the scheduled time.</li> </ul>                                                                                                                                                                                                     |

| Button                 | Description                 |
|------------------------|-----------------------------|
| <b>Next</b>            | Displays the next page.     |
| <b>Back</b>            | Displays the previous page. |
| <b>Generate Report</b> | Generates the report.       |
| <b>Cancel</b>          | Cancels your action.        |

---

## Editing report parameters

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Generation**.
3. Select the report whose parameters you want to edit.
4. Click **Edit**.
5. On the Edit Report Definition page, edit the required parameters.
6. Click **Generate Report** to generate a report.

---

## Rerunning reports

### About this task

Use rerun reports to generate a new report after Communication Manager synchronization is complete. Rerunning reports displays the latest available data after synchronization.

Using the rerun feature, you can run the reports according to the previous configuration of the report.

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Generation**.
3. On the Reports Generation page, select the report that you want to rerun.
4. Click **Run Now**.

The system displays a status message that the report generation is scheduled.

After the system generates the report, the Report Generation page displays the date of report creation.

---

## Customizing reports

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the left navigation pane, click **Generation**.
3. On the Reports Generation page, do one of the following actions:
  - Click **New**.
  - Select a report, and click **Edit**.

The system directs you to the New Report page.

4. On the New Report page, select one or more Communication Manager instances.
5. Click **Next**.

The system directs you to the **Basic Report**.

6. In the **Basic Report** section, select one or more Communication Manager instances and do one of the following actions:
  - Select **Basic (List and Display)**, and do the following actions:
    - a. Select the type of report from **Report Type**.
    - b. Select **Communication Manager Objects** that you want the report to display.
    - c. Select one or more Communication Manager instances.
  - Select **Detailed (Database)**, and perform the following actions:
    - a. Select the report type from **Report Type**.
    - b. Select one or more instances from the **Available Fields** column.
    - c. Click the right arrow to add one or more instances from the **Available Fields** column to the **Selected Fields** column.

The **Selected Fields** table displays the selected columns. Some columns are available by default in the **Selected Fields** table.

7. Click **Next**.

The system displays the Report Parameters page.

8. In the **Customize Report** field, select the **Customize Report Header** to add a name of your choice to the report.
9. Select **Export Column Titles on First Row** to export the column titles that the system displays on the report output.
10. On the Report Parameters page, complete the report parameters, and click **Generate Report**.

You can download and view the report from **Services > Reports > History**.

---

## Downloading reports

### Before you begin

You must generate a report by clicking **Services > Reports > Generation**.

If you select multiple reports and download them, the files are archived and downloaded as a zip file.

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **History**.
3. Perform one of the following actions:
  - From the **Reports History** table, select the report you want to download and click **Download Report**.
  - In the **Reports History** table, click the hyperlink in the **File Name** column.

The report is downloaded to your local computer.

### Related links

[Reports History field descriptions](#) on page 1091

## Reports History field descriptions

| Name                          | Description                                                                                                                                                                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b>              | The name you type while generating a report.                                                                                                                                                                                                                                                   |
| <b>Format</b>                 | The format in which the report is generated.                                                                                                                                                                                                                                                   |
| <b>Creation Date</b>          | The date of creating the generated report.                                                                                                                                                                                                                                                     |
| <b>Created By</b>             | The name of the user who generated the report.                                                                                                                                                                                                                                                 |
| <b>Object/CM Command Used</b> | <p>The Communication Manager command that you use to create this report.</p> <ul style="list-style-type: none"> <li>• For Basic Reports, the column shows the Communication Manager command used.</li> <li>• For Detailed Reports, the column shows the <b>Object</b> command used.</li> </ul> |
| <b>File Size</b>              | The size of the report file in KB.                                                                                                                                                                                                                                                             |

| Button                 | Description                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Download Report</b> | Downloads the selected report to your local computer.                                                                                                            |
| <b>Email Report</b>    | Displays the Email Report page to enter one or more email addresses to send the report history. You can enter multiple email addresses separated by a semicolon. |
| <b>Delete</b>          | Displays the Report History Delete Confirmation page to delete the selected report.                                                                              |

### Related links

[Downloading reports](#) on page 1090

## Configuring email properties

### About this task

Use this procedure to set up the email configuration for receiving email notifications from System Manager instances.

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR**.
3. On the View Profile:SMGR page, click **Edit**.
4. On the Edit Profile:SMGR page, in the Email Configuration Properties section, do the following.
  - a. In the **Enable email notification** field, type `true`.

- b. In the respective fields, type the appropriate values.

For more information, see “View and Edit Profile SMGR field descriptions.”

5. Click **Commit**.

---

## Sending reports through email

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **History**.
3. Select the report or reports that you want to send through email.
4. Click **Email Report**.
5. In the **Enter email addresses** field, enter the email addresses to send the report.  
You can enter multiple email addresses separated by a semicolon.
6. Click **Email Report**.  
To go to the previous page, click **Back**.  
To clear the entered email addresses, click **Clear**.

---

## Deleting reports

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **History**.
3. From the **Reports History** table, select the report that you want to delete.
4. Click **Delete**.
5. On the Report History Delete Confirmation page, click **Delete**.

---

## Configuring report properties

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > Reports > Configuration**.

3. Click **Edit**.
4. On the Edit Profile:Configuration page, configure the following:
  - Alarm Properties
  - Cleanup Properties
  - Output Directory Properties
5. Click **Commit**.

#### Related links

[View Profile:Configuration field descriptions](#) on page 869

---

## Remote server configuration

---

### Adding a remote server

#### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Reports > Remote Server Configuration**.
3. On the Remote Server Configuration page, click **New**.
4. On the Add Server page, complete the remote server details.
5. Click **Commit**.

---

### Viewing the details of a remote server

#### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Reports > Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server to view its details.
4. Click **View**.

You can view the remote server details on the View Server page.

---

## Editing the details of a remote server

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Reports > Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server to edit its details.
4. Click **Edit**.
5. On the Edit Server page, edit the remote server details.
6. Click **Commit**.

---

## Deleting a remote server

### Procedure

1. On the System Manager web console, click **Services > Reports**.
2. In the navigation pane, click **Reports > Remote Server Configuration**.
3. On the Remote Server Configuration page, select the server or servers that you want to delete.
4. Click **Delete**.
5. On the Confirmation page, click **Delete**.

---

## Add Server field descriptions

| Name                    | Description                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------|
| <b>Name</b>             | The name of the remote server.                                                                  |
| <b>IP Address</b>       | The IP address of the remote server.                                                            |
| <b>Server Path</b>      | The remote server path where the reports are saved.                                             |
| <b>Type</b>             | The type of remote server: <ul style="list-style-type: none"><li>• SCP</li><li>• SFTP</li></ul> |
| <b>Default Library</b>  | The option to use the default library to store the reports.                                     |
| <b>User Name</b>        | The user name of the remote server.                                                             |
| <b>Password</b>         | The password of the remote server.                                                              |
| <b>Confirm Password</b> | The remote server password to retype.                                                           |



| Button        | Description                                     |
|---------------|-------------------------------------------------|
| <b>Commit</b> | Adds or edits the changes to the remote server. |
| <b>Clear</b>  | Clears all changes that you perform.            |
| <b>Cancel</b> | Cancels your current action.                    |
| <b>Edit</b>   | Edits the remote server configuration details.  |
| <b>Done</b>   | Saves the remote server configuration changes.  |

## Remote Server Configuration field descriptions

| Name                  | Description                                                                                        |
|-----------------------|----------------------------------------------------------------------------------------------------|
| <b>Name</b>           | The name of the remote server.                                                                     |
| <b>IP</b>             | The IP address of the remote server.                                                               |
| <b>Type</b>           | The type of remote server: <ul style="list-style-type: none"> <li>• SCP</li> <li>• SFTP</li> </ul> |
| <b>Default Server</b> | The default server.                                                                                |
| <b>Creation Date</b>  | The date of creating the remote server.                                                            |

| Button        | Description                                                                    |
|---------------|--------------------------------------------------------------------------------|
| <b>New</b>    | Displays the Add Server page to add a new remote server.                       |
| <b>Edit</b>   | Displays the Edit Server page to edit the remote server configuration details. |
| <b>View</b>   | Displays the View Server page to view the remote server configuration details. |
| <b>Delete</b> | Deletes the selected remote server.                                            |

# Chapter 18: Managing scheduled jobs

---

## Scheduler

The Scheduler service provides a generic job scheduling service for System Manager and Avaya Aura® applications. The Scheduler service provides an interface to run a job on demand or on a periodic basis. You can schedule a job to generate an output immediately or set the frequency of the task execution to run on a periodic basis. You can modify the frequency for a periodic job schedule any time. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled jobs can be of three types:

- **System scheduled:** The job that the system executes on a periodic basis for the system to operate normally. The system adds these jobs at start-up and supports all frequencies other than one time. Scheduled jobs run asynchronously in the background. As an administrator, you cannot add or delete system-scheduled jobs. You can only disable or enable the jobs to stop temporarily.
- **Admin scheduled:** The job that the administrator schedules for administering the application. The administrator can use various navigation paths to schedule jobs such as bulk import and directory synchronization. The system lists the jobs in the scheduler as admin scheduled jobs.
- **On-demand:** The administrator can schedule on-demand jobs from the list of existing jobs.

You can perform the following operations using the Scheduler page on System Manager Web Console:

- View the pending and completed scheduled jobs.
- Modify a job scheduled by an administrator or an on-demand job.
- Delete a scheduled job.
- Schedule an on-demand job.
- Stop a running job.
- Enable or disable a job.
- Search a scheduled job.

By default, the following jobs are in **Enabled** state after System Manager is installed.

- **LogPurgeRule**

- **CirdAlarmPurgeRule**
- **AgedAlarmPurgeRule**

For a better system performance, ensure that these jobs remain in an **Enabled** state.

 **Note:**

It is recommended not to disable the above jobs manually. If you find the above jobs in a **Disabled** state, change their state to **Enabled**. For more information on “Enabling a job”, see [Enabling a job](#) on page 1102.

---

## Functions of the User Management scheduled job

Using the User Management scheduled job, you can:

- Notify users about the communication profile credentials of newly created UPM user.
- Notify users about the login credentials of newly created user.
- Notify users about the reset communication profile password.
- Notify users about their service or account inactivity and the date when it will be disabled.
- Notify users about their service or account disabled status.
- Notify users about account locked status.
- Notify users about password change or reset.
- Notify users about communication profile password change or reset.
- Warn users about password expiration.
- Notify users about expired password status.

---

## Accessing scheduler

### Procedure

On the System Manager web console, click **Services > Scheduler**.

---

## Assigning permissions to access Scheduler

### About this task

System Manager provides access permissions to Scheduler through Role Based Access Control (RBAC). System Manager defines flexible access privileges for add, delete, modify, view, schedule

on-demand, enable, disable and stop. With the privileges, users with administrator credentials can create custom roles.

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
  - Click **New**.
  - Right-click and select **New**.

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.

4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select a group.
8. In **Element or Resource Instance**, select **adminSched**, **onDemand**, **sysSched**, or **All**.
9. Click **Next**.
10. Select all operations, and click **Commit**.

You can now gain access to the **Scheduler** links.

---

## Viewing pending jobs

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. In the navigation pane, click **Pending Jobs**.
3. To view the details of the job, on the Pending Jobs page, select a pending job and click **View**.

The Job Scheduling-View Job page displays the details of the selected job.

### Related links

[Pending Jobs field descriptions](#) on page 1103

---

## Viewing completed jobs

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. Click **Completed Jobs** in the left navigation pane.  
The Completed Jobs page displays completed jobs.
3. To view the details of the jobs, on the Completed Jobs page, select a completed job and click **View**.

The Job Scheduling-View Job page displays the details of the selected job.

### Related links

[Completed Jobs field descriptions](#) on page 1105

---

## Viewing logs for a job

### About this task

Use this functionality to view logs for a pending and completed job.

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. Perform the following:
  - To view logs for a pending job, click **Pending Jobs**, select a pending job, and click **More Actions > View Log**.
  - To view logs for a completed job, click **Completed Jobs**, select a completed job, and click **More Actions > View Log**.

The log viewer displays the details for the selected job.

---

## Filtering jobs

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. Perform one of the following:
  - To filter pending jobs, click **Scheduler > Pending Jobs**, and click **Filter: Enable**.
  - To filter completed jobs, click **Scheduler > Completed Jobs**, and click **Filter: Enable**.

The system displays the **Filter: Enable** option at the upper-right corner of the page.

3. Complete the fields to filter a job using the following criteria:
  - **Job Type**. The type of the job.
  - **Job Name**. Name of the job.
  - **Job Status**. Status of the job.
  - **State**. State of the job.
  - **Frequency**. Frequency at which the job must be executed.
  - **Scheduled By**. The user who scheduled the job
4. Click **Apply**.

The system displays jobs that match the filter criteria.

---

## Editing a job

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. Perform one of the following steps:
  - To edit a pending job, click **Pending Jobs**, select a pending job, and click **Edit** or click **View > Edit**.
  - To edit a completed job, click **Completed Jobs**, select a pending job, and click **Edit** or click **View > Edit**.
3. On the Job Scheduling-Edit Job page, modify the appropriate information and click **Commit** to save the changes.

You can modify information in the following fields: **Job Name**, **Job State** in the Job Details sections, and **Task Time**, **Recurrence**, **Range** in the Job Frequency section.

---

## Deleting a job

### Before you begin

Ensure that you have logged in as an administrator to delete an administrator scheduled job.

### About this task

Use this functionality to delete an obsolete job. You can delete an on-demand and an administrator scheduled job.

#### **Note:**

You can remove only **Schedule On Demand** type of jobs.

## Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. To remove a pending job, click **Pending Jobs** in the left navigation pane.
  - a. On the Pending Jobs page, select a pending job.
    - If the job that you want to delete is currently running then you must stop the job. To stop the job, click **More Actions > Stop**.
    - If the job that you want to delete is in the enabled state, disable the job. See [Disabling a job](#) on page 1101 on how to disable a job.
  - b. Click **Delete**.
  - c. On the Delete Confirmation page, click **OK**.  
System Manager deletes the selected job from the database.
3. To remove a completed job, click **Completed Jobs** in the left navigation pane.
  - a. On the Completed Jobs page, select a completed job.  
If the job that you want to delete is in the enabled state, disable the job.
  - b. Click **Delete**.
  - c. On the Delete Confirmation page, click **OK**.  
System Manager deletes the selected job from the database.

---

## Disabling a job

### About this task

Use this functionality to make a job inactive.

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. To disable a pending job, click **Pending Jobs** in the left navigation pane.
  - a. On the Pending Jobs page, select a pending job and click **More Actions > Disable**.
  - b. On the Disable Confirmation page, click **Continue**.  
The **State** of the selected job changes to **Disabled**.
3. To disable a completed job, click **Completed Jobs** in the left navigation pane.
  - a. On the Completed Jobs page, select a completed job and click **More Actions > Disable**.
  - b. On the Disable Confirmation page, click **Continue**.  
The **State** of the selected job changes to **Disabled**.

---

## Enabling a job

### About this task

Use this functionality to make a job active.

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. To enable a pending job, perform the following steps:
  - a. Click **Pending Jobs** in the left navigation pane.
  - b. On the Pending Jobs page, select a pending job and click **More Actions > Enable**.

The system displays `Enabled` in the **State** column of the selected job.

3. To enable a completed job, perform the following steps:
  - a. Click **Completed Jobs** in the left navigation pane.
  - b. On the Completed Jobs page, select a completed job and click **More Actions > Enable**.

 **Note:**

When you enable a job, the system does not restart the job that completed all executions. To restart a job that completed all executions, reconfigure the job parameters from Job Scheduling-Edit Job page.

The system displays `Enabled` in the **State** column of the selected job.

---

## Stopping a job

### Procedure

1. On the System Manager web console, click **Services > Scheduler**.
2. In the navigation pane, click **Pending Jobs**.
3. On the Pending Jobs page, select a pending job in the running state and click **More Actions > Stop**.
4. Click **Continue** on the Stop Confirmation page.

Scheduler stops the selected job.



## Pending Jobs field descriptions

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Type</b>     | The type of job represented by a job type icon. The types of job with icons are: <ol style="list-style-type: none"> <li>1.  System scheduled job.</li> <li>2.  Admin scheduled job.</li> <li>3.  On-demand job.</li> </ol> |
| <b>Job Name</b>     | The name of the scheduled job.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Job Status</b>   | The current status of the pending job. The types of status are: <ol style="list-style-type: none"> <li>1. Pending Execution</li> <li>2. Running</li> </ol>                                                                                                                                                                                                                                                                                                                    |
| <b>State</b>        | The state of a job whether the job is active or inactive. The types of state are: <ul style="list-style-type: none"> <li>• Enabled: An active job.</li> <li>• Disabled: An inactive job.</li> </ul>                                                                                                                                                                                                                                                                           |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Scheduled By</b> | The person who scheduled the job.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Element</b>      | The element name for which the job is executed. For example, Communication Manager and its IP, if the job is for some specific Communication Manager.                                                                                                                                                                                                                                                                                                                         |

| Button                                          | Description                                                                                                             |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>View</b>                                     | Displays the Job Scheduling-View Job page that displays the details of the selected pending job.                        |
| <b>Edit</b>                                     | Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected pending job.         |
| <b>Delete</b>                                   | Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected jobs.                    |
| <b>More Actions &gt; View Log</b>               | Displays the Logging page that displays the logs for the selected pending jobs.                                         |
| <b>More Actions &gt; Stop</b>                   | Stops the selected job that is currently running.                                                                       |
| <b>More Actions &gt; Enable</b>                 | Changes the state of the selected pending job from inactive to active.                                                  |
| <b>More Actions &gt; Disable</b>                | Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected pending job.           |
| <b>More Actions &gt; Schedule On Demand Job</b> | Displays the Job Scheduling-On Demand Job page that you can use to schedule the selected pending job of type On Demand. |

*Table continues...*

| Button                 | Description                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Advanced Search</b> | Displays fields that you can use to specify the search criteria for searching a pending job.                               |
| <b>Filter: Enable</b>  | Displays fields under select columns that you can use to set filter criteria.<br><b>Filter: Enable</b> is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria.<br><b>Filter: Disable</b> is a toggle button.        |
| <b>Filter: Apply</b>   | Filters pending jobs based on the filter criteria.                                                                         |
| <b>Select: All</b>     | Selects all the pending jobs in the table displayed in the <b>Job List</b> section.                                        |
| <b>Select: None</b>    | Clears the selection for the pending jobs that you have selected.                                                          |
| <b>Refresh</b>         | Refreshes the pending job information.                                                                                     |

### Criteria section

To view this section, click **Advanced Search**. You can find the **Advanced Search** link at the at the upper-right corner of the page.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | The following three fields: <ul style="list-style-type: none"> <li>• Field 1– The list of criteria that you can use to search the pending jobs.</li> <li>• Field 2 – The operators for evaluating the expression. The operators displayed depends on the type of criterion that you selected in the first field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Button        | Description                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Clear</b>  | Clears the search value that you entered in the third field.                                                                     |
| <b>Search</b> | Searches the pending jobs based on the specified search conditions and displays the search results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancels the search operation and hides the <b>Criteria</b> section.                                                              |

### Related links

[Viewing pending jobs](#) on page 1098

[Scheduler](#) on page 1096

## Completed Jobs field descriptions

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Type</b>     | The type of job represented by a job type icon. The types of job with icons are: <ol style="list-style-type: none"> <li>1.  System scheduled job.</li> <li>2.  Admin scheduled job.</li> <li>3.  On-demand job.</li> </ol> |
| <b>Job Name</b>     | The name of the scheduled job.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Job Status</b>   | The current status of the pending job. The types of status are: <ol style="list-style-type: none"> <li>1. Status Unknown</li> <li>2. Interrupted</li> <li>3. Failed</li> <li>4. Successful</li> <li>5. Not Authorized</li> </ol>                                                                                                                                                                                                                                              |
| <b>Last Run</b>     | The date and time when the job was last run.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>State</b>        | The state of a job, whether the job is active or inactive. The types of state are: <ul style="list-style-type: none"> <li>• Enabled: An active job.</li> <li>• Disabled: An inactive job.</li> </ul>                                                                                                                                                                                                                                                                          |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Scheduled By</b> | The person who scheduled the job.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Button                                          | Description                                                                                                       |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>View</b>                                     | Displays the Job Scheduling-View Job page that displays the details and of the selected completed job.            |
| <b>Edit</b>                                     | Displays the Job Scheduling-Edit Job page that you can use to modify the information of a selected completed job. |
| <b>Delete</b>                                   | Displays the Delete Confirmation page that prompts you to confirm the deletion of the selected Jobs.              |
| <b>More Actions &gt; View Log</b>               | Displays the Logging page that displays the logs for the selected completed jobs.                                 |
| <b>More Actions &gt; Enable</b>                 | Changes the state of the selected completed job from inactive to active.                                          |
| <b>More Actions &gt; Disable</b>                | Displays the Disable Confirmation page that prompts you to confirm the disabling of the selected completed job.   |
| <b>More Actions &gt; Schedule On Demand Job</b> | Displays the Job Scheduling-On Demand Job page that you can use to schedule an On Demand job.                     |

*Table continues...*

| Button                 | Description                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Advanced Search</b> | Displays fields that you can use to specify the search criteria for searching a completed job.         |
| <b>Filter: Enable</b>  | Displays fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button.         |
| <b>Filter: Apply</b>   | Filters pending jobs based on the filter criteria.                                                     |
| <b>Select: All</b>     | Selects all the completed jobs in the table displayed in the Job List section.                         |
| <b>Select: None</b>    | Clears the selection for the completed jobs that you have selected.                                    |
| <b>Refresh</b>         | Refreshes the completed job information.                                                               |

### Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link at the at the upper-right corner of the page.

| Name            | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>Displays the following three fields:</p> <ul style="list-style-type: none"> <li>• Field 1 - The list of criteria that you can use to search the completed jobs.</li> <li>• Field 2 – The operators for evaluating the expression. The operators that system displays depends on the type of criterion that you selected in the first field.</li> <li>• Field 3 – The value corresponding to the search criteria.</li> </ul> |

| Button        | Description                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Clear</b>  | Clears the search value that you entered in the third field.                                                                       |
| <b>Search</b> | Searches the completed jobs based on the specified search conditions and displays the search results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancels the search operation and hides the <b>Criteria</b> section.                                                                |

### Related links

[Viewing completed jobs](#) on page 1099

[Scheduler](#) on page 1096

---

## Job Scheduling-View Job field descriptions

Use this page to view the details and frequency of a job.

## Job Details

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Name</b>   | The name of the job.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Job Type</b>   | The type of job represented by a job type icon. The types of job with icons are: <ol style="list-style-type: none"> <li>1.  System scheduled job.</li> <li>2.  Admin scheduled job.</li> <li>3.  On-demand job.</li> </ol> |
| <b>Job Status</b> | The current status of the job. The types of status are: <ol style="list-style-type: none"> <li>1. Running</li> <li>2. Pending</li> <li>3. Status Unknown</li> <li>4. Interrupted</li> <li>5. Failed</li> <li>6. Successful</li> <li>7. Not Authorized</li> </ol>                                                                                                                                                                                                              |
| <b>Job State</b>  | The state of a job whether the job is active or inactive. The types of state are: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> An active job.</li> <li>• <b>Disabled:</b> An inactive job.</li> </ul>                                                                                                                                                                                                                                                             |

## Job Frequency

| Name              | Description                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Task Time</b>  | The date and time of running the job.                                                                                                                                                       |
| <b>Recurrence</b> | The settings that define whether the execution of the jobs is a recurring activity or a one-time activity. In case of a recurring job, the field also displays the frequency of recurrence. |
| <b>Range</b>      | The number of recurrences or a date after which the job stops to recur.                                                                                                                     |

| Button          | Description                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------|
| <b>View Log</b> | Displays the Logging page that you can use to view the logs for the selected job.               |
| <b>Edit</b>     | Displays the Job Scheduling-Edit Job page that you can use to edit the pending job information. |
| <b>Cancel</b>   | Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page. |

## Related links

[Scheduler](#) on page 1096

## Job Scheduling-Edit Job field descriptions

### Job Details

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Name</b>     | The name of the job.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Job Type</b>     | <p>The type of job represented by a job type icon. The types of job with icons are:</p> <ol style="list-style-type: none"> <li>1.  System scheduled job.</li> <li>2.  Admin scheduled job.</li> <li>3.  On-demand job.</li> </ol> <p> <b>Note:</b><br/>You can only view the information in this field.</p> |
| <b>Job Status</b>   | <p>The current status of the job. The types of status are:</p> <ol style="list-style-type: none"> <li>1. Running</li> <li>2. Pending</li> <li>3. Status Unknown</li> <li>4. Interrupted</li> <li>5. Failed</li> <li>6. Successful</li> <li>7. Not Authorized</li> </ol> <p> <b>Note:</b><br/>You can only view the information in this field.</p>                                                                                                                                                                                                            |
| <b>Job State</b>    | <p>The state of a job whether the job is active or inactive. The types of state are:</p> <ul style="list-style-type: none"> <li>• Enabled: An active job.</li> <li>• Disabled: An inactive job.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Scheduled By</b> | <p>The scheduler of the job.</p> <p> <b>Note:</b><br/>You can only view the information in this field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Job Frequency

| Name             | Description                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Task Time</b> | The date and time of running the job. Use the calendar icon to select a date. The time is in the HH:MM:SS format followed by PM and AM. |

*Table continues...*

| Name              | Description                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recurrence</b> | The settings that define whether the execution of the jobs is a recurring activity or a one-time activity. In case of a recurring job, the field displays the frequency of recurrence. |
| <b>Range</b>      | The number of recurrences or the date after which the job stops to recur.                                                                                                              |

| Button        | Description                                                                                     |
|---------------|-------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves the changes to the database.                                                              |
| <b>Cancel</b> | Closes the Job Scheduling-View Job page and returns to the Pending Jobs or Completed Jobs page. |

**Related links**

[Scheduler](#) on page 1096

---

## Job Scheduling-On Demand Job field descriptions

Use this page to schedule an on-demand job.

**Job Details**

| Name            | Description          |
|-----------------|----------------------|
| <b>Job Name</b> | The name of the job. |

**Job Frequency**

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Task Time</b>  | The date and time of running the job.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Recurrence</b> | <p>The settings that define whether the execution of the jobs is a recurring activity or a one-time activity. In case of a recurring job, the field also display the time interval of recurrence. The options are:</p> <ul style="list-style-type: none"> <li>• Execute task one time only.</li> <li>• Task are repeated: <ul style="list-style-type: none"> <li>- Minutes</li> <li>- Hourly</li> <li>- Daily</li> <li>- Weekly</li> <li>- Yearly</li> </ul> </li> </ul> |

*Table continues...*

| Name          | Description                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Range</b>  | The settings that define the number of recurrences or date after which the job stops recurring. The options are: <ul style="list-style-type: none"> <li>• No End Date</li> <li>• End After occurrences</li> <li>• End By Date</li> </ul> |
| Button        | Description                                                                                                                                                                                                                              |
| <b>Commit</b> | Schedules an On-Demand job.                                                                                                                                                                                                              |
| <b>Cancel</b> | Cancels the scheduling of an On Demand job operation and returns to the Pending Jobs or Completed Jobs page.                                                                                                                             |

## Disable Confirmation field descriptions

Use this page to disable selected jobs.

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Type</b>   | The type of job represented by a job type icon. The types of job with icons are: <ol style="list-style-type: none"> <li>1.  System scheduled job.</li> <li>2.  Admin scheduled job.</li> <li>3.  On-demand job.</li> </ol> |
| <b>Job Name</b>   | The name of the scheduled job.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Job Status</b> | The current status of the pending job. The types of status are: <ol style="list-style-type: none"> <li>1. Running</li> <li>2. Pending</li> <li>3. Status Unknown</li> <li>4. Interrupted</li> <li>5. Failed</li> <li>6. Successful</li> <li>7. Not Authorized</li> </ol>                                                                                                                                                                                                            |
| <b>State</b>      | The state of a job whether the job is active or inactive. The types of state are: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> An active job.</li> <li>• <b>Disabled:</b> An inactive job.</li> </ul>                                                                                                                                                                                                                                                                   |

*Table continues...*



| Name                | Description                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Run</b>     | The date and time when the job was last run successfully.<br><br>* <b>Note:</b><br>The last run is applicable only for completed jobs. |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.                                                                       |
| <b>Scheduled By</b> | The scheduler of the job.                                                                                                              |

| Button          | Description                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------|
| <b>Continue</b> | Disables the job and cancels the next executions that are scheduled for the job.            |
| <b>Cancel</b>   | Cancels the operation of disabling a job and returns to the Pending or completed Jobs page. |

**Related links**

[Scheduler](#) on page 1096

---

## Stop Confirmation field descriptions

Use this page to stop a running job.

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Type</b>   | The type of job represented by a job type icon. The types of job with icons are:<br><br>1.  System scheduled job.<br><br>2.  Admin scheduled job.<br><br>3.  On-demand job. |
| <b>Job Name</b>   | The name of the scheduled job.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Job Status</b> | The current status of the pending job. The jobs on this page have status Running.                                                                                                                                                                                                                                                                                                                                                    |
| <b>State</b>      | The state of a job whether the job is active or inactive. The types of state are:<br><br>• <b>Enabled:</b> An active job.<br><br>• <b>Disabled:</b> An inactive job.<br><br>All the jobs on this page are in the <b>Enabled</b> state.                                                                                                                                                                                               |

*Table continues...*

| Name                | Description                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Run</b>     | The date and time when the job was last run successfully.<br><br>* <b>Note:</b><br>The last run is applicable only for completed jobs. |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.                                                                       |
| <b>Scheduled By</b> | The scheduler of the job.                                                                                                              |

| Button          | Description                                                                   |
|-----------------|-------------------------------------------------------------------------------|
| <b>Continue</b> | Stops the job.                                                                |
| <b>Cancel</b>   | Cancels the operation of stopping a job and returns to the Pending Jobs page. |

**Related links**

[Scheduler](#) on page 1096

---

## Delete Confirmation field descriptions

| Name                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Type</b>     | The type of job represented by a job type icon. The types of job with icons are: <ol style="list-style-type: none"> <li>1.  System scheduled job.</li> <li>2.  Admin scheduled job.</li> <li>3.  On-demand job.</li> </ol> |
| <b>Job Name</b>     | The name of the scheduled job.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Job Status</b>   | The current status of the job.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>State</b>        | The state of a job whether the job is active or inactive. The types of state are: <ul style="list-style-type: none"> <li>• <b>Enabled:</b> An active job.</li> <li>• <b>Disabled:</b> An inactive job.</li> </ul> The jobs on this page are in the <b>Disabled</b> state.                                                                                                                                                                                                           |
| <b>Last Run</b>     | The date and time when the job was last run.<br><br>* <b>Note:</b><br>The last run is applicable only for completed jobs.                                                                                                                                                                                                                                                                                                                                                           |
| <b>Frequency</b>    | The time interval between two consecutive executions of the job.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Scheduled By</b> | The scheduler of the job.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Button   | Description                                                                                |
|----------|--------------------------------------------------------------------------------------------|
| Continue | Deletes the selected job.                                                                  |
| Cancel   | Cancels the operation of deleting a job and returns to the Pending or completed Jobs page. |

**Related links**

[Scheduler](#) on page 1096

# Chapter 19: Templates

---

## Template management

A template is a file that contains stored settings. You can use templates to streamline the process of performing various routine activities. Templates save the data that you enter so that you can perform similar activities later without re-entering the same data. With System Manager, you can create, store, and use templates to simplify tasks like adding, editing, and viewing endpoints or subscribers. In System Manager, you can use default templates or you can create your own templates as well.

Templates are available in two categories: default templates and user-defined templates. The default templates exist on the system and you cannot edit or remove them. You can, however, modify or remove user-defined or custom templates any time.

You can create a custom alias endpoint template by duplicating a default alias template. The Alias template is populated in **Custom templates** after synchronization. You can view, edit, upgrade and delete these alias custom templates in **Templates > CM Endpoint > Custom templates**.

---

## Template versioning

### Template versioning

You can version endpoint templates with Communication Manager 5.0 and later. You can associate a template with a specific version of an adopting product through template versioning. You can use the **Template Version** field under endpoint templates to accommodate endpoint template versioning.

You can also use template versioning for subscriber templates using the following versions: Aura Messaging 6.3, Aura Messaging 6.2, Aura Messaging 6.1, Aura Messaging 6.0, MM 5.0, MM 5.1, MM 5.2, CMM 5.2, CMM 6.0, CMM 6.2, CMM 6.3 and CMM 7.0.

---

## Filtering templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.

2. Click either **Endpoint** or **Messaging** for endpoint templates and messaging templates respectively.
3. Select the Communication Manager or supported messaging version, whichever applicable.
4. Click **Show List**.
5. Click **Filter: Enable** in the Template List.
6. Filter the endpoint or subscriber templates according to one or multiple columns.
7. Click **Apply**.

To hide the column filters, click **Disable**. This does not clear any filter criteria that you have set.

 **Note:**

The table displays only those endpoint or subscriber templates that match the filter criteria.

---

## Upgrading a template

Use this feature to upgrade an existing Communication Manager template to a later Communication Manager release. You can upgrade only custom templates. This feature supports upgrading a Communication Manager agent or endpoint template from an earlier Communication Manager release to a subsequent Communication Manager release. You can also upgrade templates across multiple releases.

This feature does not support downgrading of template versions.

When you perform the upgrade operation, note that:

- System migrates the existing template settings to the new template version.
- System sets the new parameters in the new template version to default values.
- System deletes the deleted parameters in the new template version as compared to the older template version.
- System makes the new keywords available for editing within the new template, but the upgraded template retains the previous keyword setting, if available. If the previous keyword is not available, then the default is used in the upgraded template.

After you commit a template upgrade task, the system upgrades the template and enlists the newly upgraded template on the Template List.

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. Click **CM Endpoint** in the left navigation pane.

3. Select the Communication Manager system whose custom template you want to upgrade from the list under **Supported Feature Server Versions**.

You can upgrade only custom templates.

4. Click **Show List**.
5. Select the custom template that you want to upgrade from **Template List**.
6. Click **Upgrade**.
7. On the Upgrade Endpoint Template page, select the Communication Manager version for template upgrade from the list in **Supported CM Version**.
8. In the **Template Name** text box, enter the new name for the template.
9. Click **Upgrade**. The system updates **Template List** with the newly upgrade template.

---

## Adding CM Agent template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Agent**.
3. Click **New**.
4. Enter a name in the **Template Name** field.
5. Complete the mandatory fields under the **General Options** and **Agents Skills** tabs.
6. Click **Commit**.

### Related links

[Add Agent Template field descriptions](#) on page 1126

---

## Editing CM Agent template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Agent**.
3. Select the template you want to edit from the Templates List.

 **Note:**

You cannot edit default templates.

4. Click **Edit** or click **View > Edit**.

5. Complete the **Edit Agent Template** page.
6. Click **Commit** to save the changes.

**Related links**

[Add Agent Template field descriptions](#) on page 1126

---

## Viewing CM Agent template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Agent**.
3. Select the template you want to view from the Templates List.
4. Click **View**.

You can view the **General Options** and **Agent Skills** sections on the View Agent Template page.

**Related links**

[Add Agent Template field descriptions](#) on page 1126

---

## Deleting CM Agent template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Agent**.
3. Select the template you want to delete from the Templates List.

 **Note:**

You cannot delete default templates.

4. Click **Delete**.

---

## Duplicating CM Agent template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Agent**.

3. Select the template you want to copy from the Templates List.
4. Click **Duplicate**.
5. Complete the **Duplicate Agent Template** page.
6. Click **Commit**.

#### Related links

[Add Agent Template field descriptions](#) on page 1126

---

## Adding CM Endpoint templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Click the **Custom Templates List** tab.
4. Click **New**.
5. Select the **Set type**.
6. Enter a name in the **Template Name** field.
7. Complete the mandatory fields under the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Dialing**, **Enhanced Call Fwd** and **Button Assignment** sections.
8. Click **Commit**.

#### Related links

[New Endpoint / Template field descriptions](#) on page 735

---

## Editing CM Endpoint templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom templates** tab.

#### **Note:**

You cannot edit default templates.



6. Select the template you want to edit from the template list.
7. Click **Edit** or click **View > Edit**.
8. Complete the **Edit Endpoint Template** page.
9. Click **Commit** to save the changes.

**Related links**

[New Endpoint / Template field descriptions](#) on page 735

---

## Viewing CM Endpoint templates

**Procedure**

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom template** or **Default template** tab.
6. Select the template you want to view.
7. Click **View**.

You can view the **General Options**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, and **Button Assignment** sections on the View Endpoint Template page.

**Related links**

[New Endpoint / Template field descriptions](#) on page 735

---

## Deleting CM Endpoint templates

**Procedure**

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom templates** tab.

 **Note:**

You cannot delete default templates.

6. Select the endpoint templates you want to delete from the endpoint template list.
7. Click **Delete**.

---

## Duplicating CM Endpoint templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **CM Endpoint**.
3. Select one or more Communication Manager instance from the Communication Manager list.
4. Click **Show List**.
5. Click the **Custom templates** tab or the **Default templates** tab.
6. Select the template you want to copy from the endpoint template list.
7. Click **Duplicate**.
8. Enter the name of the new template in the **New Template Name** field.
9. Choose the appropriate set type from the **Set Type** field.
10. Complete the **Duplicate Endpoint Template** page and click **Commit**.

### Related links

[New Endpoint / Template field descriptions](#) on page 735

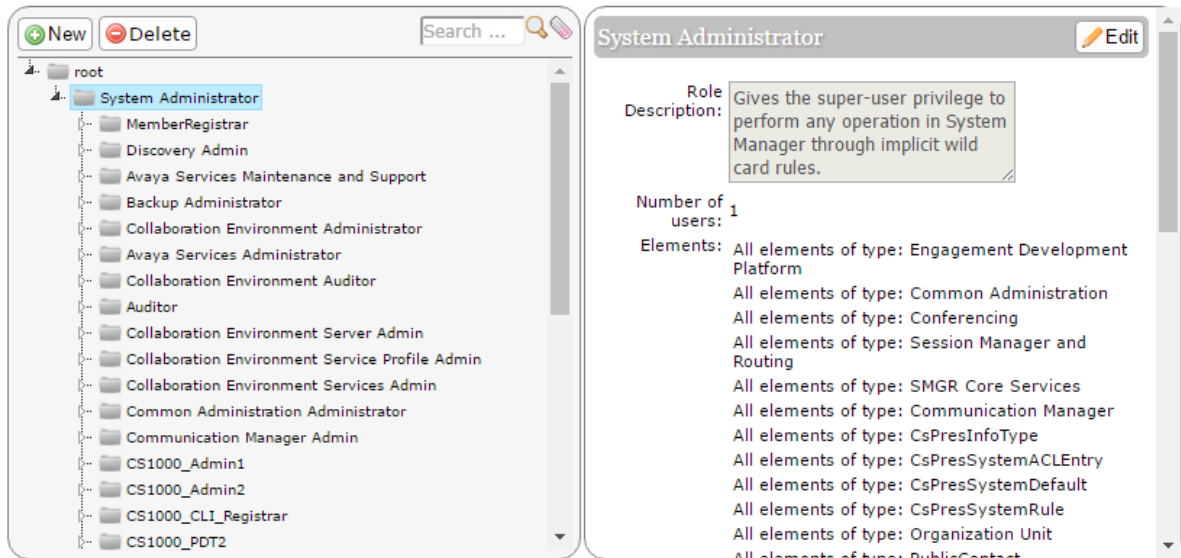
---

## Assigning permissions for CM templates

### Procedure

1. On the System Manager web console, click **Users > Groups & Roles**.
2. In the navigation pane, click **Roles**.
3. On the Roles page, select an existing role, and perform one of the following steps:
  - Click **New**
  - Right-click and select **New**.

The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.



4. On the Add New Role page, type the name and the description for the role.
5. Click **Commit and Continue**.
6. Click **Add Mapping**.
7. In **Group Name**, select the group of templates to which you want to apply this permission.  
You can leave **Group Name** blank if you do not want to select a group.
8. In the **Element or Resource Type** field, click **Communication Manager Templates**.
9. In the **Element or Resource Instance** field, click the Communication Manager templates to which you want to apply this permission.

The system displays only the templates you select in the **Element or Resource Instance** field in the Agent or Endpoints Templates List page.

10. Click **Next**.
11. On the Permission Mapping page, apply the required permission. For example, click **select view**.
12. Click **Commit**.

Users with the view permission can only view the CM Endpoint templates within the specified group. You must select **All** and then select view.

## Adding subscriber templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **Messaging**.

3. Select a messaging version from the list of supported messaging versions.
4. Click **Show List**.
5. Click **New**.
6. Complete the **Basic Information**, **Subscriber Directory**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous** sections in the Add Subscriber Template page.
7. Click **Commit**.

Subscriber templates have different versions based on the software version. The subscriber templates you create have to correspond to the Avaya Aura® Messaging, Modular Messaging, or Communication Manager Messaging software version. When you select a messaging template, the **Software Version** field in the Add Subscriber Template page displays the appropriate version information.

#### Related links

[Subscriber MM Templates field descriptions](#) on page 1137  
[Subscriber CMM Templates field descriptions](#) on page 1135  
[Subscriber Messaging Templates field descriptions](#) on page 1132

---

## Editing subscriber templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **Messaging**.
3. From the supported messaging version list, select a messaging version.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **Edit** or **View > Edit**.
7. Edit the required fields on the **Edit Subscriber Template** page.
8. Click **Commit** to save the changes.

#### **Note:**

You cannot edit any of the default subscriber templates.

#### Related links

[Subscriber MM Templates field descriptions](#) on page 1137  
[Subscriber CMM Templates field descriptions](#) on page 1135  
[Subscriber Messaging Templates field descriptions](#) on page 1132

---

## Viewing subscriber templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **Messaging**.
3. From the supported messaging versions list, select one of the messaging versions.
4. Click **Show List**.
5. Select a subscriber template from the Subscriber Template list.
6. Click **View** to view the mailbox settings of this subscriber.

 **Note:**

You cannot edit any of the fields in the View Subscriber Template page.

### Related links

[Subscriber MM Templates field descriptions](#) on page 1137

[Subscriber CMM Templates field descriptions](#) on page 1135

[Subscriber Messaging Templates field descriptions](#) on page 1132

---

## Deleting subscriber templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a supported messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the templates you want to delete.
6. Click **Delete**.

 **Note:**

You cannot delete any default subscriber template.

---

## Duplicating subscriber templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **Messaging**.

3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select the subscriber template you want to copy.
6. Click **Duplicate**.
7. Complete the Duplicate Subscriber Template page and click **Commit**.

#### Related links

[Subscriber MM Templates field descriptions](#) on page 1137  
[Subscriber CMM Templates field descriptions](#) on page 1135  
[Subscriber Messaging Templates field descriptions](#) on page 1132

---

## Viewing associated subscribers

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **Messaging**.
3. From the list of supported messaging versions, select a messaging version.
4. Click **Show List**.
5. From the Subscriber Template list, select a subscriber template for which you want to view the associated subscribers.
6. Click **More Actions > View Associated Subscribers**.

You can view all the associated subscribers in the System Manager database for the template you have chosen in the Associated Subscribers page.

---

## Templates List

You can view Templates List when you click **Template** under **Services** on the System Manager console.

You can apply filters and sort each of the columns in the Template List. When you click **Refresh**, you can view the updated information available after the last synchronization operation.

### IP Office Endpoint Templates

| Name | Description           |
|------|-----------------------|
| Name | Name of the template. |

*Table continues...*

| Name                      | Description                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System Type</b>        | The name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template. |
| <b>Version</b>            | The change version of the template.                                                                                                                                                                    |
| <b>Set Type</b>           | The set type of the branch gateway endpoint template.                                                                                                                                                  |
| <b>Last Modified Time</b> | The time and date when the template was last modified.                                                                                                                                                 |

| Name                                     | Description                                                                                                                                                                                            |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                              | The name of the template.                                                                                                                                                                              |
| <b>Owner</b>                             | The name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template. |
| <b>Version</b>                           | The change version of the template.                                                                                                                                                                    |
| <b>Default</b>                           | Specifies whether the template is default or user-defined.                                                                                                                                             |
| <b>Last Modified</b>                     | The time and date when the endpoint or messaging template was last modified.                                                                                                                           |
| <b>Set type</b> (for endpoint templates) | The set type of the endpoint template.                                                                                                                                                                 |
| <b>Type</b> (for messaging templates)    | Specifies whether the messaging type is Messaging, MM, or CMM.                                                                                                                                         |
| <b>Software Version</b>                  | The software version of the element for the template.                                                                                                                                                  |

### IP Office System Configuration template

| Name                      | Description                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>               | Name of the template.                                                                                                                                                                                  |
| <b>System Type</b>        | The name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template. |
| <b>Version</b>            | The change version of the template.                                                                                                                                                                    |
| <b>Last Modified Time</b> | The time and date when the template was last modified.                                                                                                                                                 |

### CM Agent template

| Name           | Description                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>    | Name of the template.                                                                                                                                                                                  |
| <b>Owner</b>   | The name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template. |
| <b>Version</b> | The change version of the template.                                                                                                                                                                    |
| <b>Default</b> | Specifies whether the template is default or user-defined.                                                                                                                                             |

*Table continues...*

| Name                    | Description                                            |
|-------------------------|--------------------------------------------------------|
| <b>Software Version</b> | The software version of the element for the template.  |
| <b>Last Modified</b>    | The time and date when the template was last modified. |

### CM Endpoint template

| Name                    | Description                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>             | Name of the template.                                                                                                                                                                                  |
| <b>Owner</b>            | The name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template. |
| <b>Version</b>          | The change version of the template.                                                                                                                                                                    |
| <b>Default</b>          | Specifies whether the template is default or user-defined.                                                                                                                                             |
| <b>Software Version</b> | The software version of the element for the template.                                                                                                                                                  |
| <b>Last Modified</b>    | The time and date when the template was last modified.                                                                                                                                                 |

### Messaging template

| Name                    | Description                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>             | Name of the template.                                                                                                                                                                                  |
| <b>Owner</b>            | The name of the user who owns a template. For default templates, System is considered to be the owner. For user-defined templates, this field specifies the name of the user who created the template. |
| <b>Version</b>          | The change version of the template.                                                                                                                                                                    |
| <b>Default</b>          | Specifies whether the template is default or user-defined.                                                                                                                                             |
| <b>Type</b>             | The type of the messaging template.                                                                                                                                                                    |
| <b>Software Version</b> | The software version of the element for the template.                                                                                                                                                  |
| <b>Last Modified</b>    | The time and date when the template was last modified.                                                                                                                                                 |

---

## Add Agent Template field descriptions

| Name                    | Description                                                                          |
|-------------------------|--------------------------------------------------------------------------------------|
| <b>System Type</b>      | The Communication Manager that the agent is assigned to.                             |
| <b>Template Name</b>    | The name of the agent template. You can enter the name of your choice in this field. |
| <b>Software Version</b> | The Communication Manager version of the agent template.                             |



| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AAS</b>                       | <p>The option to use this extension as a port for an Auto Available Split/Skill. By default, this check box is clear. This option is intended for communication server adjunct equipment ports only, not human agents.</p> <p> <b>Important:</b></p> <p>When you enter <i>y</i> in the AAS field, it clears the password and requires execution of the <b>remove agent-loginid</b> command. To set AAS to <i>n</i>, remove this logical agent, and add it again.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>ACW Agent Considered Idle</b> | <p>The option to count After Call Work (ACW) as idle time. The valid entries are <b>System</b>, <b>Yes</b>, and <b>No</b>. Select <b>Yes</b> to have agents who are in ACW included in the Most-Idle Agent queue. Select <b>No</b> to exclude ACW agents from the queue.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>AUDIX</b>                     | <p>The option to use this extension as a port for AUDIX. By default, this check box is clear.</p> <p> <b>Note:</b></p> <p>The AAS and AUDIX fields cannot both be <i>y</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>AUDIX Name for Messaging</b>  | <p>You have the following options:</p> <ul style="list-style-type: none"> <li>• Enter the name of the messaging system used for LWC Reception</li> <li>• Enter the name of the messaging system that provides coverage for this Agent LoginID</li> <li>• Leave the field blank. This is the default setting.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Auto Answer</b>               | <p>When using EAS, the auto answer setting of the agent applies to the station where the agent logs in. If the auto answer setting for that station is different, the agent setting overrides the station setting. The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>all</b>: Immediately sends all ACD and non-ACD calls to the agent. The station is also given a single ring while a non-ACD call is connected. You can use the ringer-off button to prevent the ring when the feature-related system parameter, <b>Allow Ringer-off with Auto-Answer</b> is set to <i>y</i>.</li> <li>• <b>acd</b>: Only ACD split /skill calls and direct agent calls go to auto answer. If this field is <i>acd</i>, non-ACD calls terminated to the agent ring audibly.</li> <li>• <b>none</b>: All calls terminated to this agent receive an audible ringing. This is the default setting.</li> <li>• <b>station</b>: Auto answer for the agent is controlled by the auto answer field on the Station screen.</li> </ul> |

*Table continues...*

| Name                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aux Work Reason Code Type</b>            | <p>Determines how agents enter reason codes when entering AUX work. The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>system:</b> Settings assigned on the Feature Related System Parameters screen apply. This is the default setting.</li> <li>• <b>none:</b> You do not want an agent to enter a reason code when entering AUX work.</li> <li>• <b>requested:</b> You want an agent to enter a reason code when entering AUX mode but do not want to force the agent to do so. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to <i>y</i>.</li> <li>• <b>forced:</b> You want to force an agent to enter a reason code when entering AUX mode. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to <i>y</i>.</li> </ul> |
| <b>Call Handling Preference</b>             | <p>Determines which call an agent receives next when calls are in queue. When calls are in queue and an agent becomes available, the following entries are valid:</p> <ul style="list-style-type: none"> <li>• <b>skill-level:</b> Delivers the oldest, highest priority calls waiting for the highest-level agent skill.</li> <li>• <b>greatest-need:</b> Delivers the oldest, highest priority calls waiting for any agent skill.</li> <li>• <b>percent-allocation:</b> Delivers a call from the skill that will otherwise deviate most from its administered allocation. Percent-allocation is available only with Avaya Business Advocate software.</li> </ul> <p>For more information, see <i>Avaya Business Advocate User Guide</i>.</p>                                                                                                                        |
| <b>COR</b>                                  | <p>The Class Of Restriction for the agent. Valid entries range from <b>0</b> to <b>995</b>. The default entry is <b>1</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Coverage Path</b>                        | <p>The coverage path number used by calls to the LoginID. Valid entries are a path number from <b>1</b> to <b>999</b>, time of day table <b>t1</b> to <b>t999</b>, or blank (default). This is used when the agent is logged out, busy, or does not answer calls.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Direct Agent Calls First (not shown)</b> | <p>The option to direct agent calls to override the percent-allocation call selection method and be delivered before other ACD calls. Clear the check box if you want to treat direct agent calls as other ACD calls. This field replaces the Service Objective field when percent-allocation is entered in the Call Handling Preference field. For more information, see <i>Avaya Business Advocate User Guide</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Direct Agent Skill</b>                   | <p>The number of the skill used to handle Direct Agent calls. Valid entries range from <b>1</b> to <b>2000</b>, or blank. The default setting is blank.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

*Table continues...*

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Forced Agent Logout Time</b>     | Enables the Forced Agent Logout by Clock Time feature by administering a time of day to automatically log out agents using an hour and minute field. Valid entries for the hour field range from <b>01</b> to <b>23</b> . Valid entries for the minute field are <b>00</b> , <b>15</b> , <b>30</b> , and <b>45</b> . The default is blank (not administered). Examples are: 15:00, 18:15, 20:30, 23:45.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Local Call Preference</b>        | The option to administer Local Preference Distribution to handle agent-surplus conditions, call-surplus conditions, or both. Use this field to administer call-surplus conditions. To set up an algorithm for agent-surplus conditions, set the Local Agent Preference field on the Hunt Group screen. You can select this check box only if the Call Center Release field is set to 3.0 or later and the Multiple Locations customer option is active.                                                                                                                                                                                                                                                                                                                                                 |
| <b>LoginID for ISDN/SIP Display</b> | The option to include the Agent LoginID CPN and Name field in ISDN and SIP messaging over network facilities. By default, the check box is clear, indicating that the physical station extension CPN and Name is sent. Send Name on the ISDN Trunk Group screen prevents sending the calling party name and number if set to n and may prevent sending it if set to r (restricted).                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Logout Reason Code Type</b>      | Determines how agents enter reason codes. The valid entries are: <ul style="list-style-type: none"> <li>• <b>System:</b> Settings assigned on the Feature Related System Parameters screen apply. This is the default entry.</li> <li>• <b>Requested:</b> You want an agent to enter a reason code when logging out but do not want to force the agent to do this. To enter this value, the reason codes and EAS on the System-Parameters Customer-Options screen must be set to y.</li> <li>• <b>Forced:</b> You want to force an agent to enter a reason code when logging out. To enter this value, the Reason Codes and EAS on the System-Parameters Customer-Options screen must be set to y.</li> <li>• <b>None:</b> You do not want an agent to enter a reason code when logging out.</li> </ul> |
| <b>LWC Reception</b>                | Indicates whether the terminal can receive Leave Word Calling (LWC) messages. The valid entries are: <ul style="list-style-type: none"> <li>• <b>audix</b></li> <li>• <b>msa-spe.</b> This is the default entry.</li> <li>• <b>none</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>LWC Log External Calls</b>       | Determines whether or not unanswered external call logs are available to end users. When external calls are not answered, Communication Manager keeps a record of up to 15 calls provided information on the caller identification is available. Each record consists of the latest call attempt date and time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Name                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum time agent in ACW before logout (Sec)</b> | <p>Sets the maximum time the agent can be in ACW on a per agent basis. The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>system:</b> This is the default entry. Settings assigned on the Feature Related System Parameters screen apply.</li> <li>• <b>none:</b> ACW timeout does not apply to this agent.</li> <li>• <b>30-9999 sec:</b> Indicates a specific timeout period. This setting will take precedence over the system setting for maximum time in ACW.</li> </ul> |
| <b>MIA Across Skills</b>                             | <p>The valid entries are:</p> <ul style="list-style-type: none"> <li>• <b>System:</b> The system-wide values apply. This is the default value.</li> <li>• <b>Yes:</b> Removes an agent from the MIA queues for all the splits or skills for which an agent is available when the agent answers a call from any assigned splits or skills.</li> <li>• <b>No:</b> Excludes ACW agents for the queue.</li> </ul>                                                                                     |
| <b>Localized Display Name</b>                        | The name associated with the agent login ID                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Attribute</b>                                     | The attribute associated with the agent login ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Percent Allocation</b>                            | <p>The percentage for each of the agent's skills if the call handling preference is percent-allocation. Valid entry is a number from <b>1</b> to <b>100</b> for each skill. Entries for all the agent skills together must add up to 100%. Do not use target allocations for reserve skills. Percent Allocation is available as part of the Avaya Business Advocate software.</p>                                                                                                                 |
| <b>Password</b>                                      | <p>The password the agent must enter upon login. Displayed only if both the AAS and AUDIX check boxes are clear. Valid entries are digits from <b>0</b> through <b>9</b>. Enter the minimum number of digits in this field specified by the Minimum Agent-LoginID Password Length field on the Feature-Related System Parameters screen. By default, this field is blank.</p>                                                                                                                     |
| <b>Confirm Password</b>                              | <p>Confirms the password the Agent entered in the Password field during login. Displayed only if both the AAS and the AUDIX check boxes are clear. By default, this field is blank.</p> <p> <b>Note:</b></p> <p>Values entered in this field are not echoed to the screen.</p>                                                                                                                                 |
| <b>Port Extension</b>                                | <p>The assigned extension for the AAS or AUDIX port. The values are displayed only if either the AAS or AUDIX check box is selected. This extension cannot be a VDN or an Agent LoginID. By default, this field is blank</p>                                                                                                                                                                                                                                                                      |

*Table continues...*

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reserve Level</b>     | <p>The reserve level to be assigned to the agent for the skill with the Business Advocate Service Level Supervisor feature or the type of interruption with the Interruptible AUX Work feature. You can assign a reserve level of 1 or 2 or an interruptible level of a, m, n, or blank for no reserve or interruptible level, where,</p> <ul style="list-style-type: none"> <li>• a: auto-in-interrupt</li> <li>• m: manual-in-interrupt</li> <li>• n: notify-interrupt</li> </ul> <p>Changes to this field take effect the next time the agent logs in. Values of 1 and 2 are allowed only if Business Advocate is enabled. A skill level cannot be assigned with a reserve level setting. Reserve level set to 1 or 2 defines the EWT threshold level for the agent to be added to the assigned skill as a reserve agent. When the EWT for this skill reaches the corresponding threshold set on the Hunt Group screen, agents automatically get this skill added to their logged in skills. Agents are delivered calls from this skill until the skill's EWT drops below the assigned overload threshold for that level. The Interruptible Aux feature is a way to help meet service level targets by requesting agents who are on break to become available when the service level target is not being met. For more information on Service Level Supervisor, see <i>Avaya Business Advocate User Guide</i>.</p> |
| <b>Service Objective</b> | <p>The option to administer Service Objective. Service Objective is administered on the Hunt Group screen and the agent LoginID screen. This field is displayed only when Call Handling Preference is set to greatest-need or skill-level. The communication server selects calls for agents according to the ratio of Predicted Wait Time (PWT) or Current Wait Time (CWT) and the administered service objective for the skill. Service Objective is part of the Avaya Business Advocate software.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Security Code</b>     | <p>The security code required by users for specific system features and functions, including the following: Personal Station Access, Redirection of Calls Coverage Off-Net, Leave Word Calling, Extended Call Forwarding, Station Lock, Message Retrieval, Terminal Self-Administration, and Demand Printing. The required security code length is administered system-wide.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Table continues...

| Name                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Skill Number</b>  | <p>The Skill Hunt Groups that an agent handles. The same skill may not be entered twice. You have the following options:</p> <ul style="list-style-type: none"> <li>• If EAS-PHD is not optioned, enter up to four skills.</li> <li>• If EAS-PHD is optioned, enter up to 20 or 60 skills depending on the platform.</li> </ul> <p> <b>Important:</b></p> <p>Assigning a large number of skills to agents can potentially impact system performance. Review system designs with the ATAC when a significant number of agents have greater than 20 skills per agent.</p> |
| <b>Skill Level</b>   | A skill level for each of an agent's assigned skills. If you specify the EAS-PHD option, 16 priority levels are available. If you do not specify this option, two priority levels are available.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Tenant Number</b> | <p>The tenant partition number. Valid entries range from <b>1</b> to <b>100</b>. The default is entry is <b>1</b>.</p> <p> <b>Note:</b></p> <p>Values entered in this field are not echoed to the screen.</p>                                                                                                                                                                                                                                                                                                                                                           |

| Button        | Description                                                       |
|---------------|-------------------------------------------------------------------|
| <b>Commit</b> | Completes the action you initiate.                                |
| <b>Clear</b>  | Clears all entries.                                               |
| <b>Done</b>   | Completes your current action and returns to the subsequent page. |
| <b>Cancel</b> | Cancels your current action and returns to the previous page.     |

## Subscriber Messaging Templates field descriptions

| Name                    | Description                                           |
|-------------------------|-------------------------------------------------------|
| <b>Template name</b>    | The template of this subscriber template.             |
| <b>Type</b>             | The messaging type of the subscriber template.        |
| <b>Software Version</b> | The software version of the element for the template. |

### Basic Information

| Name              | Description                       |
|-------------------|-----------------------------------|
| <b>Last Name</b>  | The last name of the subscriber.  |
| <b>First Name</b> | The first name of the subscriber. |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PBX Extension</b>         | <p>A number whose length can range from three digits to 10 digits, that the subscriber will use to log on to the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The Extension Number must:</p> <ul style="list-style-type: none"> <li>• Be within the range of Extension Numbers assigned to your system.</li> <li>• Not be assigned to another local subscriber.</li> <li>• Be a valid length on the local computer.</li> </ul> |
| <b>Password</b>              | <p>The default password that users must use to log on to their mailbox.</p> <p>The password must be from 3 to 15 digits and adhere to system policies that you set on the Avaya Aura® Messaging server.</p>                                                                                                                                                                                                                                                                             |
| <b>Class Of Service Name</b> | <p>The Class Of Service (CoS) name for this subscriber.</p> <p>CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.</p>                                                                                                                                                                                                                                            |
| <b>Community ID</b>          | <p>The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.</p>                                                                                                                                                                                                                                                                                                                |

## Subscriber Directory

| Name                         | Description                                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Telephone Number</b>      | The name that the system displays before the computer name and domain in the subscriber's email address.                                  |
| <b>Common Name</b>           | The display name of the subscriber.                                                                                                       |
| <b>ASCII version of name</b> | If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name. |

## Mailbox Features

| Name                              | Description                                                                                                                                                                                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personal Operator Mailbox</b>  | The mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting. |
| <b>Personal Operator Schedule</b> | Specifies when to route calls to the backup operator mailbox. The default value for this field is <b>Always Active</b> .                                                                                                              |

*Table continues...*

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TUI Message Order</b> | <p>The order in which the subscriber hears the voice messages. The options are:</p> <ul style="list-style-type: none"> <li>• <b>urgent first then newest:</b> to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• <b>oldest messages first:</b> to direct the system to play messages in the order they were received.</li> <li>• <b>urgent first then oldest:</b> to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</li> <li>• <b>newest messages first:</b> to direct the system to play messages in the reverse order of how they were received.</li> </ul> |
| <b>Intercom Paging</b>   | <p>The intercom paging settings for a subscriber. The options are:</p> <ul style="list-style-type: none"> <li>• <b>paging is off:</b> To disable intercom paging for this subscriber.</li> <li>• <b>paging is manual:</b> If the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber.</li> <li>• <b>paging is automatic:</b> If the TUI automatically allows callers to page the subscriber.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>VoiceMail Enabled</b> | <p>Specifies whether a subscriber can receive messages, email messages, and call-answer messages from other subscribers. The options are:</p> <ul style="list-style-type: none"> <li>• <b>yes:</b> use this to create, forward, and receive messages.</li> <li>• <b>no:</b> to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.</li> </ul>                                                                                                                                                                                                                                                                                                                    |

## Secondary Extensions

| Name                       | Description                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secondary extension</b> | The number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension. |

## Miscellaneous

| Name                  | Description                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Miscellaneous1</b> | Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Miscellaneous2</b> | Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |

*Table continues...*



| Name                  | Description                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Miscellaneous3</b> | Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Miscellaneous4</b> | Gives additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the messaging system. |

| Button                | Description                                             |
|-----------------------|---------------------------------------------------------|
| <b>Commit</b>         | Adds the subscriber template.                           |
| <b>Reset or Clear</b> | Undoes all the changes.                                 |
| <b>Edit</b>           | Allows you to edit the fields.                          |
| <b>Done</b>           | Completes your action and returns to the previous page. |
| <b>Cancel</b>         | Returns to the previous page.                           |
| <b>Schedule</b>       | Performs the action at the chosen time.                 |

## Subscriber CMM Templates field descriptions

| Name                     | Description                                                                |
|--------------------------|----------------------------------------------------------------------------|
| <b>Template name</b>     | The template of this subscriber template.                                  |
| <b>New Template Name</b> | The name of the duplicate template. You can enter the name of your choice. |
| <b>Type</b>              | The messaging type of the subscriber template.                             |
| <b>Software Version</b>  | The software version of the element for the template.                      |

### Basic Information

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>  | The last name of the subscriber.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>First Name</b> | The first name of the subscriber.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Extension</b>  | <p>A number that is between 3-digits and 10-digits in length, that the subscriber will use to log into the mailbox. Other local subscribers can use the Extension Number to address messages to this subscriber. The extension number must:</p> <ul style="list-style-type: none"> <li>• Be within the range of Extension Numbers assigned to your system.</li> <li>• Not be assigned to another local subscriber.</li> <li>• Be a valid length on the local computer.</li> </ul> |
| <b>Password</b>   | The default password that a user has to use to login to his or her mailbox. The password you enter can be 1 to 15 digits in length and cannot be blank                                                                                                                                                                                                                                                                                                                            |

*Table continues...*

| Name                       | Description                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Class Of Service ID</b> | The class of service (CoS) ID for this subscriber.<br><br>CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system.                                                                                                                      |
| <b>Community ID</b>        | The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1.                                                                                                                                                                                        |
| <b>MWI Enabled</b>         | The option to set the message waiting indicator (MWI) for the subscriber. The options are: <ul style="list-style-type: none"> <li>• <b>No:</b> If the system must not send MWI for the subscriber or if the subscriber does not have a phone or switch on the network.</li> <li>• <b>Yes:</b> If the system must send MWI for the subscriber.</li> </ul> |
| <b>Account Code</b>        | The Subscriber Account Code. The Subscriber Account Code is used to create Call Detail Records on the switch for calls placed by the voice ports. The value you enter in this field can contain any combination of digits from 0 to 9. If an account code is not specified, the system will use the subscriber's mailbox extension as the account code.  |

### Subscriber Directory

| Name                | Description                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------|
| <b>Email Handle</b> | The name that the system displays before the computer name and domain in the subscriber's email address. |
| <b>Common Name</b>  | The display name of the subscriber.                                                                      |

### Mailbox Features

| Name                      | Description                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Covering Extension</b> | The number to be used as the default destination for the Transfer Out of Messaging feature. You can enter 3 to 10 digits depending on the length of the system extension, or leave this field blank. |

### Secondary Extensions

| Name                       | Description                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secondary extension</b> | The number assigned to a subscriber for receiving fax messages. Valid Entries are blank or 3-10 digits (0-9), depending on the length of the system's extension. |

### Miscellaneous

| Name          | Description                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Misc 1</b> | Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system. |

*Table continues...*

| Name          | Description                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Misc 2</b> | Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system. |
| <b>Misc 3</b> | Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system. |
| <b>Misc 4</b> | Additional, useful information about a subscriber. Entries in this field are for convenience and are not used by the Messaging system. |

| Button                | Description                                            |
|-----------------------|--------------------------------------------------------|
| <b>Commit</b>         | Adds the subscriber template.                          |
| <b>Reset or Clear</b> | Undoes all changes.                                    |
| <b>Edit</b>           | Allows you to edit the fields.                         |
| <b>Done</b>           | Completes the action and returns to the previous page. |
| <b>Cancel</b>         | Returns to the previous page.                          |

## Subscriber MM Templates field descriptions

| Name                     | Description                                                                |
|--------------------------|----------------------------------------------------------------------------|
| <b>Type</b>              | The messaging type of the subscriber template.                             |
| <b>New Template Name</b> | The name of the duplicate template. You can enter the name of your choice. |
| <b>Template name</b>     | The messaging template of a subscriber template.                           |
| <b>Software Version</b>  | The software version of the element for the template.                      |

### Basic Information

| Name                       | Description                                                                                                                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Name</b>           | The last name of the subscriber.                                                                                                                                                                                                    |
| <b>First Name</b>          | The first name of the subscriber.                                                                                                                                                                                                   |
| <b>Numeric Address</b>     | A unique address in the voice mail network. The numeric address can be from 1 to 50 digits and can contain the Mailbox Number.                                                                                                      |
| <b>PBX Extension</b>       | The primary telephone extension of the subscriber.                                                                                                                                                                                  |
| <b>Class Of Service ID</b> | The class of service (CoS) ID for this subscriber.<br><br>CoS controls subscriber access to many features and provides general settings, such as mailbox size. The value that you select must be available in the messaging system. |

*Table continues...*

| Name                | Description                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Community ID</b> | The default community ID for the subscriber. Community IDs are used to control message sending and receiving among groups of subscribers. The default value is 1. |
| <b>Password</b>     | The default password the subscriber must use to log in to his or her mailbox. The password can be from one digit in length to a maximum of 15 digits.             |

### Subscriber Directory

| Name                         | Description                                                                                                                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Email Handle</b>          | The name that the system displays before the computer name and domain in the subscriber's e-mail address. The computer name and domain are automatically added to the handle you enter when the subscriber sends or receives an e-mail.                                                           |
| <b>Telephone Number</b>      | The telephone number of the subscriber as displayed in address book listings and client applications. The entry can be a maximum of 50 characters in length and can contain any combination of digits (0-9), period (.), hyphen (-), plus sign (+), and left and right parentheses (()) and (()). |
| <b>Common Name</b>           | The display name of the subscriber in address book listings, such as those for e-mail client applications. The name you enter can be 1 to 64 characters in length. This field is automatically populated when you add a new subscriber.                                                           |
| <b>ASCII Version of Name</b> | If the subscriber name is entered in multi-byte character format, then this field specifies the ASCII translation of the subscriber name.                                                                                                                                                         |

### Mailbox Features

| Name                              | Description                                                                                                                                                                                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Backup Operator Mailbox</b>    | The mailbox number or transfer dial string of the subscriber's personal operator or assistant. This field also indicates the transfer target when a caller to this subscriber presses 0 while listening to the subscriber's greeting. |
| <b>Personal Operator Schedule</b> | Specifies when to route calls to the backup operator mailbox. The default value for this field is <b>Always Active</b> .                                                                                                              |

*Table continues...*

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TUI Message Order</b> | <p>The order in which the subscriber hears the voice messages. You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>urgent first then newest:</b> to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the reverse order of how they were received.</li> <li>• <b>oldest messages first:</b> to direct the system to play messages in the order they were received.</li> <li>• <b>urgent first then oldest:</b> to direct the system to play any messages marked as urgent prior to playing non-urgent messages. Both the urgent and non-urgent messages are played in the order of how they were received.</li> <li>• <b>newest messages first:</b> to direct the system to play messages in the reverse order of how they were received.</li> </ul> |
| <b>Intercom Paging</b>   | <p>The intercom paging settings for a subscriber. You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>paging is off:</b> to disable intercom paging for this subscriber.</li> <li>• <b>paging is manual:</b> if the subscriber can modify, with Subscriber Options or the TUI, callers can page the subscriber.</li> <li>• <b>paging is automatic:</b> if the TUI automatically allows callers to page the subscriber.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Voicemail Enabled</b> | <p>Specifies whether a subscriber can receive messages, e-mail messages and call-answer messages from other subscribers. You can choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>yes:</b> use this to create, forward, and receive messages.</li> <li>• <b>no:</b> to prevent the subscriber from receiving call-answer messages and to hide the subscriber from the telephone user interface (TUI). The subscriber cannot use the TUI to access the mailbox, and other TUI users cannot address messages to the subscriber.</li> </ul>                                                                                                                                                                                                                                                                                                                    |

## Secondary Extensions

| Name                       | Description                                                                                                                                                                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secondary extension</b> | <p>Specifies one or more alternate number to reach a subscriber. You can use secondary extensions to specify a telephone number for direct reception of faxes, to allow callers to use an existing Caller Application, or to identify each line appearance on the subscriber's telephone set if they have different telephone numbers.</p> |

## Miscellaneous

| Name          | Description                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Misc 1</b> | Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 2</b> | Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 3</b> | Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |
| <b>Misc 4</b> | Gives additional, useful information about a subscriber template. Entries in this field are for convenience and are not used by the messaging system. |

| Button        | Description                                             |
|---------------|---------------------------------------------------------|
| <b>Commit</b> | Adds the subscriber template.                           |
| <b>Reset</b>  | Undoes all the changes.                                 |
| <b>Edit</b>   | Allows you to edit the fields.                          |
| <b>Done</b>   | Completes your action and returns to the previous page. |
| <b>Cancel</b> | Returns to the previous page.                           |

## Managing IP Office Endpoint template

### Adding an IP Office endpoint template

#### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Click **New**.
4. Enter the required information in the **Name**, **System Type**, **Set Type**, and **Version** fields.
5. Click **Details**.

The system launches the IP Office Manager application.

6. On the IP Office Manager window, in the right pane, specify the required details, such as voice mail, telephony, and button programming in the respective tabs.

7. Click **File > Save Template and Exit** to save the template configuration and exit the IP Office application.

The system directs you to the landing page of **IP Office Endpoint**.

You can view the newly created template in the list of templates under IP Office endpoint templates.

When you upgrade System Manager, Default Centralized ATA Template, Default Centralized SIP Template are now available to create centralized users.

#### Related links

[IP Office endpoint template field descriptions](#) on page 1143

---

## Viewing an IP Office endpoint template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. Under **IP Office Endpoint Templates**, select the template you want to view from the list of templates.
6. Click **View**.

This action launches the IP Office Manager application.

7. On the IP Office Manager window, click the tabs on the right pane to view the template details.
8. Click **File > Exit** to exit the IP Office Manager application.

The system displays the **IP Office Endpoint** landing page.

#### Related links

[IP Office endpoint template field descriptions](#) on page 1143

---

## Editing an IP Office endpoint template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.

5. From the list of **IP Office Endpoint Templates**, select the template you want to edit.
6. Click **Edit**.  
This system launches the IP Office application.
7. On the IP Office Manager window, in the right pane, edit the required details.
8. Click **File > Save Template and Exit** to save the modifications to the template and exit the IP Office Manager application.

The system displays the IP Office Endpoint landing page.

#### Related links

[IP Office endpoint template field descriptions](#) on page 1143

---

## Duplicating an IP Office endpoint template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a system type from the list of IP Office supported templates.
4. Click **Show List**.
5. From the list of IP Office endpoint templates, select the template you want to duplicate.
6. Click **Duplicate**.
7. Type a template name in the **New Template Name** field.
8. Click **Commit**.

If you want to make changes to the new endpoint template, click **Details**.

#### Related links

[IP Office endpoint template field descriptions](#) on page 1143

---

## Deleting an IP Office endpoint template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select a type of system from the list of IP Office supported templates.
4. Click **Show List**.
5. From the **IP Office Endpoint Templates** list, select the template you want to delete.
6. Click **Delete**.



The system displays the template instance you selected for deletion.

7. Perform one of the following:

- Click **Delete** to delete the template.
- Click **Cancel** to cancel the delete operation and return to the **IP Office Endpoint** landing page.

## Upgrading IP Office endpoint templates

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office Endpoint**.
3. Select the IP Office device type.
4. Click **Show List**.
5. Select the template you want to upgrade.
6. Click **Upgrade**.
7. In the **Supported IP Office Versions** field, enter the target version for upgrade.
8. In **Template Name**, type the name of the template.

Template name must be a unique name.

9. Click **Upgrade**.

System Manager upgrades the selected template, and the IP Office Manager starts with the upgraded template. The original template you selected is retained.

10. After the IP Office Manager starts, the new, upgraded template, save and exit.

The system displays the upgraded template in the IP Office Endpoint List page.

## IP Office endpoint template field descriptions

| Name               | Description                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>        | The name of the IP Office endpoint template.                                                                                                                                                                               |
| <b>System Type</b> | The type of system associated with the IP Office device. The valid options are: <ul style="list-style-type: none"> <li>• <b>IP Office</b>: for IP Office core unit</li> <li>• <b>B5800</b>: for B5800 core unit</li> </ul> |
| <b>Version</b>     | The version of the IP Office endpoint template.                                                                                                                                                                            |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Set Type</b>           | <p>The set type associated with the IP Office endpoint template. This is a drop-down field listing the following set types:</p> <ul style="list-style-type: none"> <li>• <b>ANALOG</b></li> <li>• <b>SIP</b></li> <li>• <b>IPDECT</b></li> <li>• <b>DIGITAL</b></li> <li>• <b>H323</b></li> <li>• <b>SIP DECT</b></li> </ul> <p>Only IP Office devices support the <b>SIP DECT</b> set type.</p> |
| <b>Last Modified Time</b> | The date and time when you last modified the template.                                                                                                                                                                                                                                                                                                                                           |

| Button         | Description                                                                  |
|----------------|------------------------------------------------------------------------------|
| <b>Details</b> | Click to open the IP Office application to add or edit the template details. |

---

## Managing IP Office System Configuration template

---

### Adding an IP Office System Configuration template

#### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.
5. Click **Details**.  
The system launches the IP Office application.
6. On the Offline Configuration Creation window, click **OK**.
7. In the right pane, complete the system configuration template by filling the required fields, and click **OK**.
8. Click **File > Save Template and Exit** to save the template specifications and exit the IP Office application.

The system directs you to the IP Office System Configuration landing page where you can view the newly created system template in the IP Office System Configuration list.

---

## Viewing an IP Office System Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. On the IP Office Branch Gateway Template page, from the IP Office supported templates list, select an IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the IP Office System Configuration list.
6. Click **View**.  
The system launches the IP Office Manager application.
7. On the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only.
8. Click **File > Exit** to exit IP Office Manager.  
The system directs you to the IP Office System Configuration landing page.

---

## Editing an IP Office system configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. On the IP Office System Configuration Templates page, select an IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the IP Office System Configuration list.
6. Click **Edit**.  
The system launches the IP Office Manager application.
7. On the IP Office Manager window, edit the required configuration parameters, and click **OK**.
8. Click **File > Save Template and Exit** to save the modifications to the system configuration template and exit the IP Office Manager application.  
The system displays the IP Office System Configuration landing page.

---

## Deleting an IP Office system configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. On the IP Office Template page, select an IP Office system type.
4. Click **Show List**.
5. Select the system configuration template you want to delete from the IP Office System Configuration list.
6. Click **Delete**.

The system displays the system template instance you selected for deletion.

7. Do one of the following:
  - Click **Delete** to delete the template.
  - Click **Cancel** to cancel the delete operation, and return to the IP Office System Configuration landing page.

---

## Applying an IP Office system configuration template on an IP Office device

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. On the IP Office Template page, select an IP Office system type.
4. Click **Show List**.
5. From the IP Office System Configuration List, select the system template you want to apply to an IP Office device.
6. Click **Apply**.

You will be directed to a new page where you can select a device to apply the template.

7. From the list of IP Office devices, select the IP Office device on which you want to apply the selected IP Office system configuration template.

#### **Important:**

When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.

8. Do one of the following:

- Click **Now** to perform apply the template immediately.
- Click **Schedule** to apply the template at a specified time in **Scheduler**.
- Click **Cancel** to cancel this task and return to the IP Office System Configuration landing page.

## IP Office System Configuration template field descriptions

| Name                      | Description                                                                                                                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>               | The name of the IP Office System Configuration template.                                                                                                                                                     |
| <b>System Type</b>        | The type of system associated with the template. The options are: <ul style="list-style-type: none"> <li>• <b>IP Office</b>: for IP Office core unit</li> <li>• <b>B5800</b>: for B5800 core unit</li> </ul> |
| <b>Version</b>            | The version number of the template.                                                                                                                                                                          |
| <b>Last Modified Time</b> | The date and time when the IP Office System Configuration template was last modified.                                                                                                                        |

| Button         | Description                                                                        |
|----------------|------------------------------------------------------------------------------------|
| <b>Details</b> | Displays the IP Office application where you can add or edit the template details. |

## Manage audio files

Audio files in .WAV and .C11 formats are used in auto attendant configuration in the Auto Attendant feature in IP Office. In System Manager, you can manage .WAV and .C11 audio files from the Manage Audio page in IP Office System Configuration in Template Management. The .C11 audio file is for use in IP Office IP500V2 or the B5800 Core Unit.

To push an auto attendant file to an IP Office System Configuration template through System Manager, you must first upload the .WAV audio files using the **Upload** button in the Manage Audio page. When you upload the .WAV audio files, the corresponding .C11 audio files are automatically created. If you need to convert any .WAV audio file which does not have a corresponding .C11 audio file, or if the corresponding .C11 audio file is deleted, click the **Convert** button in the Manage Audio page.

Use the **Manage Audio** page in **IP Office System Configuration** to:

- Upload .WAV and .C11 audio files.
- Convert .WAV to .C11 audio file format.
- Delete .WAV and .C11 audio files.

---

## Uploading an audio file

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options > Manage Audio**.
4. On the Manage Audio page, enter the complete path of the audio file in the **Select an Audio File** text box. You can also click **Browse** to locate and select the audio file you want to upload.

The system displays the audio file you selected for uploading in a table.

 **Note:**

System Manager filters uploaded files based on mime type or bytes in the file. If a file type does not match, System Manager shows up an error message.

5. If you want to remove the audio file from your selection, click the **Remove** link in the **Action** column.
6. Click **Upload**.

You can view the newly uploaded audio files listed in the **List of Audio Files** table.

---

## Converting a .WAV audio file to a .C11 audio file

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options > Manage Audio**.
4. On the Manage Audio page, select the .WAV audio file from the **List of Audio Files** that you want to convert to .C11 format.
5. On the Convert Audio page, the system lists the file you selected for conversion.
6. If you want to change the recording label of the .WAV file, edit the label text in the corresponding text box under the **Recording Label** column.
7. Click **Commit** to confirm the convert action.

The system displays the newly converted audio file under the corresponding audio name column in the **List of Audio Files** table.

## Deleting an audio file

### About this task

Use the **Delete** button to delete audio files from the list of audio files. You can choose to either delete the .WAV audio format, or the .C11 audio file format, or delete both the audio file formats in a single step.

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the navigation pane, click **IP Office System Configuration**.
3. Click **More Options > Manage Audio**.
4. On the Manage Audio page, select the audio file you want to delete from the list of audio files.
5. Click **Delete**.
6. On the Delete Audio File Confirmation page, you can view the audio files you selected in Step 4 for deletion. From the **Select the type of deletion** field perform one of the following:
  - Select the type of audio file extension you want to delete.
  - Select **Both** if you want to delete both the file extension types.

Sample scenario: Suppose you have ABC.wav and ABC.c11 audio files in the **List of Audio Files**. If you want to delete only the ABC.wav audio file, then select **Wave** from **Select the type of deletion**. If you want to delete both the audio files in a single step, then select **Both** from the **Select the type of deletion** field.

7. Click **Delete**.
8. Click **Done** to return to the IP Office System Configuration landing page.

## Manage Audio field descriptions

| Name                                     | Description                                                        |
|------------------------------------------|--------------------------------------------------------------------|
| <b>wav Audio File Name</b>               | The file name of the .WAV type of audio file.                      |
| <b>Last uploaded time of wav</b>         | The time when you last uploaded the .WAV audio file in the system. |
| <b>Recording Label</b>                   | The recording label of the .wav file.                              |
| <b>C11 Audio File Name</b>               | The file name of the .C11 type of audio file.                      |
| <b>Last converted time of wav to C11</b> | The time when you last converted a .wav file to a .C11 audio file. |
| <b>Select an Audio File</b>              | Displays the complete path of the audio file.                      |

*Table continues...*

| Name                                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select the type of deletion</b> on the Delete Audio File Confirmation page | Provides the option to select the type of deletion of audio files. The valid options are: <ul style="list-style-type: none"> <li>• <b>Wave</b>: Select to delete only the .WAV type of file for the selected audio file.</li> <li>• <b>C11</b>: Select to delete only the .C11 type of file for the selected audio file.</li> <li>• <b>Both</b>: Select to delete both, .WAV and .C11, types of files for the selected audio file.</li> </ul> |

| Button                                                   | Description                                                                                 |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Delete</b>                                            | Click to delete the selected audio file.                                                    |
| <b>Convert</b>                                           | Click to convert an audio file of type .WAV to .C11.                                        |
| <b>Done</b>                                              | Click to exits the <b>Manage Audio</b> page and return to the IP Office Template List page. |
| <b>Browse</b>                                            | Click to locate and select an audio file.                                                   |
| <b>Upload</b>                                            | Click to upload an audio file to System Manager.                                            |
| <b>Delete</b> on the Delete Audio File Confirmation page | Click to confirm the delete action for the selected audio file.                             |
| <b>Cancel</b> on the Delete Audio File Confirmation page | Click to cancel the delete operation and return to the <b>Manage Audio</b> page.            |

## Managing UCM and Application Server system configuration templates

### Adding a UCM and Application Server Configuration template Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Templates List** section, click **New**.
4. Complete the **Name**, **System Type**, and **Version** fields.
5. Click **Details**.  
The system launches the IP Office Manager application.
6. On the Offline Configuration Creation window, click **OK**.



7. In the right pane, complete the system configuration template by filling the required fields, and click **OK**.
8. Click **File > Save Template and Exit** to save the template specifications and exit the IP Office Manager application.

The system directs you to the UCM and Application Server Templates landing page where you can view the newly created system template in the **UCM and Application Server Templates** list.

#### Related links

[UCM and Application Server Templates field descriptions](#) on page 1154

---

## Viewing a UCM and Application Server Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, in the **Supported System Types** section, select one of the following system types:
  - IP Office Application Server
  - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to view from the **UCM and Application Server Templates** list.
6. Click **View**.

On the IP Office Manager window, in the right pane, you can view the system configuration template details. All the fields are read-only.

The system starts the IP Office Manager application.

7. Click **File > Exit** to exit IP Office Manager.

The system displays the UCM and Application Server Templates page where you can select a device to apply the template.

#### Related links

[UCM and Application Server Templates field descriptions](#) on page 1154

---

## Editing a UCM and Application Server Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.

2. In the left navigation page, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select any one of the following system types:
  - IP Office Application Server
  - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to edit from the UCM and Application Server Templates list.
6. Click **Edit**.

The system launches the IP Office Manager application.
7. On the IP Office Manager window, edit the required configuration parameters, and click **OK**.
8. Click **File > Save Template and Exit** to save the modifications to the system configuration template and exit the IP Office Manager application.

The system displays the UCM and Application Server Templates landing page.

#### Related links

[UCM and Application Server Templates field descriptions](#) on page 1154

---

## Deleting a UCM and Application Server Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select one of the following system types:
  - IP Office Application Server
  - Unified Communications Module
4. Click **Show List**.
5. Select the system configuration template you want to delete from the UCM and Application Server Templates list.
6. Click **Delete**.

The system displays the system template instance you selected for deletion.
7. Do one of the following:
  - Click **Delete** to delete the template.
  - Click **Cancel** to cancel the delete operation, and return to the UCM and Application Server Templates landing page.

**Related links**

[UCM and Application Server Templates field descriptions](#) on page 1154

---

## Applying a UCM and Application Server Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **UCM and Application Server Configuration**.
3. On the UCM and Application Server Templates page, In the **Supported System Types** section, select one of the following system types:
  - IP Office Application Server
  - Unified Communications Module
4. Click **Show List**.
5. From the UCM and Application Server Configuration List, select the system template you want to apply to a device.
6. Click **Apply**.

You will be directed to a new page where you can select a device to apply the template.

7. From the list of IP Office devices, select the IP Office device on which you want to apply the selected UCM and Application Server Configuration template.

 **Important:**

When you apply a template on a device, the data of the template that you wish to apply may override the existing system configuration data on the device.

8. Do one of the following:
  - Click **Now** to perform apply the template immediately.
  - Click **Schedule** to apply the template at a specified time in **Scheduler**.
  - Click **Cancel** to cancel this task and return to the UCM and Application Server Templates landing page.

**Related links**

[UCM and Application Server Templates field descriptions](#) on page 1154

---

## UCM and Application Server Templates field descriptions

| Name                      | Description                                                                                                                                                                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>               | The name of the system configuration template of UCM and Application Server.                                                                                                                                                                      |
| <b>System Type</b>        | The type of system associated with the template. The options are: <ul style="list-style-type: none"><li>• <b>Unified Communications Module</b>: For UCM core unit</li><li>• <b>Application Server</b>: For Application Server core unit</li></ul> |
| <b>Version</b>            | The version number of the template.                                                                                                                                                                                                               |
| <b>Last Modified Time</b> | The date and time when the UCM and Application Server System Configuration template was last modified.                                                                                                                                            |

| Button         | Description                                                              |
|----------------|--------------------------------------------------------------------------|
| <b>Details</b> | Displays the application where you can add or edit the template details. |

---

## Managing VMPro system configuration templates

---

### Adding a VMPro System Configuration template

#### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.

The system launches the **VMPro** application.

6. In the right pane, complete the system configuration template by filling the required fields, and click **Update**.
7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

The system displays the VMPro System Configuration page where you can view the newly created system configuration template.

#### Related links

[VMPro System Configuration Templates field descriptions](#) on page 1157

---

## Viewing a VMPPro System Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPPro System Configuration Template**.
3. On the VMPPro Template page, from the **VMPPro** supported templates list, select a **VMPPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the **VMPPro** System Configuration list.
6. Click **View**.  
The system launches the **VMPPro** application.
7. On the VMPPro window, in the right pane, you can view the system configuration template details. All the fields are read-only.

### Related links

[VMPPro System Configuration Templates field descriptions](#) on page 1157

---

## Editing a VMPPro System Configuration template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPPro System Configuration Template**.
3. On the VMPPro System Configuration Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the system configuration template you want to edit from the VMPPro System Configuration list.
6. Click **Edit**.  
The system launches the VMPPro application.
7. To edit the configuration parameters on the Voicemail Pro-System Preferences window, click **Update**.
8. Click **OK**.
9. Click **File > Save and Exit** to save the modifications to the system configuration template and exit the VMPPro application.

The system displays the VMPPro System Configuration Template page.

## Related links

[VMPro System Configuration Templates field descriptions](#) on page 1157

---

# Deleting a VMPro System Configuration template

## Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro System Configuration Template**.
3. On the VMPro System Configuration Templates page, select a **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to delete from the VMPro System Configuration Template list.
6. Click **Delete**.

The system displays the system template instance you selected for deletion.

7. Do one of the following:
  - Click **Delete** to delete the template.
  - Click **Cancel** to cancel the delete operation, and return to the VMPro System Configuration Template landing page.

## Related links

[VMPro System Configuration Templates field descriptions](#) on page 1157

---

# Applying a VMPro System Configuration template on a device

## Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro System Configuration Templates**.
3. On the VMPro System Configuration Template page, select a Voicemail Pro system type.
4. Click **Show List**.
5. From the VMPro System Configuration Templates List, select the system template you want to apply to a VMPro device.
6. Click **Apply**.

The system displays the VMPro System Configuration page where you can select a device to apply the template.

7. From the list of VMPro devices, select the VMPro device on which you want to apply the VMPro system configuration template.

**! Important:**

When you apply a template on a device, the data of the template that you apply might override the existing system configuration data on the device.

8. Do one of the following:

- Click **Now** to perform apply the template immediately.
- Click **Schedule** to apply the template at a specified time in **Scheduler**.
- Click **Cancel** to cancel this task and return to the VMPro System Configuration Template landing page.

**Related links**

[VMPro System Configuration Templates field descriptions](#) on page 1157

---

## Duplicating a VMPro System Configuration template

**Procedure**

1. On the System Manager web console, click **Services > Templates**.
  2. In the left navigation pane, click **VMPro System Configuration Template**.
  3. On the VMPro System Configuration Templates page, select a VoicemailPro system type.
  4. Click **Show List**.
  5. From the VMPro System Configuration list, select the system configuration template that you want to duplicate.
  6. Click **Duplicate**.
- The system launches the VMPro application.
7. In the **New Template Name** field, type the name of the new template.
  8. Click **Commit**.

The system displays the new template on the VMPro System Configuration Templates page.

**Related links**

[VMPro System Configuration Templates field descriptions](#) on page 1157

---

## VMPro System Configuration Templates field descriptions

| Name           | Description                             |
|----------------|-----------------------------------------|
| <b>Name</b>    | The name of the Voicemail Pro template. |
| <b>Version</b> | The version number of the template.     |

*Table continues...*

| Name               | Description                                                                    |
|--------------------|--------------------------------------------------------------------------------|
| Last Modified Time | The date and time when the IP Office Voicemail Pro template was last modified. |

| Button  | Description                                                                                      |
|---------|--------------------------------------------------------------------------------------------------|
| Details | Displays the IP Office Voicemail Pro application where you can add or edit the template details. |

---

## Managing VMPro call flow templates

---

### Adding a VMPro Call Flow template

#### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. Click **New**.
4. Complete the **Name** and **Version** fields.
5. Click **Details**.  
The system launches the **VMPro** application.
6. In the right pane, complete the call flow template by filling the required fields, and click **Update**.
7. Click **Save and Exit** to save the template specifications and exit the **VMPro** application.

#### Result

The system displays the VMPro Call Flow page where you can view the newly created call flow template.

#### Related links

[VMPro Call Flow Templates field descriptions](#) on page 1161

---

### Viewing a VMPro Call Flow template

#### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.



3. On the VMPro Template page, from the **VMPro** supported templates list, select the **VMPro** system type.
4. Click **Show List**.
5. Select the system configuration template you want to view from the **VMPro** call flow list.
6. Click **View**.

### Result

The system launches the **VMPro** application. On the VMPro window, in the right pane, you can view the call flow template details. All the fields are read-only.

### Related links

[VMPro Call Flow Templates field descriptions](#) on page 1161

---

## Editing a VMPro Call Flow template

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. Select the call flow template you want to edit from the VMPro Call Flow list.
6. Click **Edit**.

The system launches the VMPro application.

7. To edit the call flow parameters on the Voicemail Pro-System Preferences window, click **Update**.
8. Click **OK**.
9. Click **File > Save and Exit** to save the modifications to the call flow template and exit the VMPro application.

### Result

The system displays the VMPro Call Flow Templates page.

### Related links

[VMPro Call Flow Templates field descriptions](#) on page 1161

---

## Deleting a VMPro Call Flow template

### Procedure

1. On the System Manager web console, click **Services > Templates**.

2. In the left navigation pane, click **VMPPro Call Flow Template**.
3. On the VMPPro Call Flow Templates page, select a **VMPPro** system type.
4. Click **Show List**.
5. Select the call flow template you want to delete from the VMPPro Call Flow Templates list.
6. Click **Delete**.

The system displays the VMPPro call flow template that you selected for deletion.

7. Do one of the following:
  - Click **Delete** to delete the template.
  - Click **Cancel** to cancel the delete operation, and return to the VMPPro Call Flow Templates page.

#### Related links

[VMPPro Call Flow Templates field descriptions](#) on page 1161

---

## Applying a VMPPro Call Flow template on a device

### Procedure

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPPro Call Flow Templates**.
3. On the VMPPro Call Flow Templates page, select the Voicemail Pro system type.
4. Click **Show List**.
5. From the VMPPro Call Flow Templates List, select the system template you want to apply to a VMPPro device.
6. Click **Apply**.

The system displays the VMPPro Call Flow page where you can select a device to apply the template.

7. From the list of VMPPro devices, select the VMPPro device on which you want to apply the VMPPro call flow template.

#### **Important:**

When you apply a template on a device, the data of the template that you apply might override the call flow data on the device.

8. Do one of the following:
  - Click **Now** to apply the template immediately.
  - Click **Schedule** to apply the template at a specified time in **Scheduler**.
  - Click **Cancel** to cancel the task and return to the VMPPro Call Flow Templates page.

**Related links**

[VMPro Call Flow Templates field descriptions](#) on page 1161

---

## Duplicating a VMPro Call Flow template

**Procedure**

1. On the System Manager web console, click **Services > Templates**.
2. In the left navigation pane, click **VMPro Call Flow Template**.
3. On the VMPro Call Flow Templates page, select a VoicemailPro system type.
4. Click **Show List**.
5. From the VMPro Call Flow list, select the call flow template that you want to duplicate.
6. Click **Duplicate**.

The system launches the VMPro application.

7. In the **New Template Name** field, type the name of the new template.
8. Click **Commit**.

**Result**

The system displays the new template on the VMPro Call Flow Templates page.

**Related links**

[VMPro Call Flow Templates field descriptions](#) on page 1161

---

## VMPro Call Flow Templates field descriptions

| Name                      | Description                                                           |
|---------------------------|-----------------------------------------------------------------------|
| <b>Name</b>               | The name of the Voicemail Pro template.                               |
| <b>Version</b>            | The version number of the template.                                   |
| <b>Last modified time</b> | The last time that the IP Office Voicemail Pro template was modified. |

| Button         | Description                                                               |
|----------------|---------------------------------------------------------------------------|
| <b>Details</b> | Displays the template details of the IP Office Voicemail Pro application. |

# Chapter 20: Security

## Extended Security Hardening

System Manager supports Standard, Commercial, and Military Grade security hardening. By default, System Manager comes with Standard Grade hardening configuration, no additional action is required to set up this configuration.

Each security hardening grade applies specific security attributes as summarized in the following table:

| Security attribute                                                                                                                                                                                                             | Standard grade | Commercial grade | Military grade       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|------------------|----------------------|
| VM Configuration Hardening <sup>1</sup>                                                                                                                                                                                        | Y              | Y                | Y                    |
| Password Management                                                                                                                                                                                                            | Y              | Y                | Y (more restrictive) |
| Login and Session Management                                                                                                                                                                                                   | Y              | Y                | Y                    |
| System and Application Files Hardening                                                                                                                                                                                         | Y              | Y                | Y                    |
| Certificate Management                                                                                                                                                                                                         | Y              | Y                | Y                    |
| Support TLS 1.2                                                                                                                                                                                                                | Y              | Y                | Y                    |
| FIPS 140-2 Compliance                                                                                                                                                                                                          | —              | Y                | Y                    |
| Multifactor Authentication (PIV and CAC support)                                                                                                                                                                               | Y              | Y                | Y                    |
| SELinux Enabled                                                                                                                                                                                                                | —              | —                | Enforced             |
| Audit Management                                                                                                                                                                                                               | Y              | Y                | Y (+ OS level audit) |
| AIDE (File Tampering Prevention)                                                                                                                                                                                               | —              | —                | Y                    |
|  <b>Note:</b><br><sup>1</sup> : VMware ESXi VMX configuration file hardening applied as part of the Solution Deployment Manager deployment. |                |                  |                      |

## Enabling Commercial Grade Hardening

### About this task

Use this procedure to enable Commercial Grade hardening.

#### ! Important:

Once you enable Commercial Grade hardening, you cannot disable it. If you want to disable Commercial Grade hardening, you must redeploy System Manager.

### Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

#### \* Note:

Delete the snapshot after the System Manager operation is complete.

### Procedure

1. Log in to the System Manager command line interface.
2. Type `setSecurityProfile --enable-commercial-grade`, and press `Enter`.
3. When the system prompts, provide the user password and press `Enter`.
4. Type one of the following and press `Enter`:
5. At the prompt, type one of the following and press `Enter`:

- 1 to continue.
- 2 to exit.

You cannot gain access to the system while the profile is being enabled.

The system takes a few minutes to complete the setting, and reboots for the changes to take effect.

6. To verify the enabled security profile, type `getSecurityprofile` and press `Enter`.

If the security profile is successfully enabled, the system displays the following message:

```
Profile Mode : commercial grade hardened mode enabled
```

```
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: permissive
```

```

Mode from config file: permissive
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28

```

FIPS State : FIPS enabled.

---

## Enabling Military Grade Hardening

### About this task

Use this procedure to enable Military Grade hardening.

#### Important:

Once you enable Military Grade hardening, you cannot disable it. If you want to disable Military Grade hardening, you must redeploy System Manager.

### Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

#### Note:

Delete the snapshot after the System Manager operation is complete.

### Procedure

1. Log in to the System Manager command line interface.
2. Type `setSecurityProfile --enable-military-grade`, and press `Enter`.
3. When the system prompts, provide the user password and press `Enter`.
4. At the prompt, type one of the following and press `Enter`:
  - 1 to continue.
  - 2 to exit.
5. At the `Enable SELinux?` prompt, type one of the following and press `Enter`:
  - 1 to enable.
  - 2 to disable.
6. At the `Enable Audit?` prompt, type one of the following and press `Enter`:
  - 1 to enable.

- 2 to disable.

7. At the `Enable AIDE Tool?` prompt, type one of the following and press `Enter`:

- 1 to enable.
- 2 to disable.

You cannot gain access to the system while the profile is being enabled.

The system takes a few minutes to complete the setting, and reboots for the changes to take effect.

8. To verify the enabled security profile, type `getSecurityprofile` and press `Enter`.

If the security profile is successfully enabled, the system displays the following message:

```
Profile Mode : military grade hardened mode enabled
```

```
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28
```

```
FIPS State : FIPS enabled.
```

```
Audit logging Enabled..
```

```
AIDE Tool Enabled..
```

## Optional settings for security hardening

To fulfil the security or environmental requirements, following are the optional settings for security hardening.

| No. | Settings                          | Reference                                                                         |
|-----|-----------------------------------|-----------------------------------------------------------------------------------|
| 1.  | Enable Out of Band Management     | <a href="#">Configuring Out of Band Management on System Manager</a> on page 1506 |
| 2.  | Modify password settings          | <a href="#">Editing password policies</a> on page 60                              |
| 3.  | Configure remote logging          | <a href="#">Configuring System Manager logs for Syslog server</a> on page 1529    |
| 4.  | Configure LDAP for authentication | <a href="#">Provisioning the LDAP server</a> on page 1241                         |
| 5.  | Configure EASG                    | <a href="#">Remote access of System Manager</a> on page 1560                      |
| 6.  | Change login banner               | <a href="#">Editing the login warning banner</a> on page 73                       |

---

## Security hardening options

System Manager provides the following security hardening options:

- selinux
- audit
- fips
- aide
- TLSv1, TLSv1.1, and TLSv1.2

You can enable or disable one or more security hardening options. While you can enable all the options, you can only disable selinux, audit, and aide.

---

## Enabling security hardening options

### About this task

Use this procedure to enable one or more security hardening options from the following:

- selinux
- audit
- fips
- aide
- TLSv1, TLSv1.1, and TLSv1.2

### Procedure

1. Log in to the System Manager command line interface.
2. Do one of the following:

- To enable only one security hardening option, type `securityHardeningOptions <security_hardening_option_name> enable`, and press Enter.

For example, type the following command, and press Enter.

```
securityHardeningOptions selinux enable
```

- To enable more than one security hardening options, type `securityHardeningOptions <Comma separated_security_hardening_option_name> enable`, and press Enter.

For example, type the following command, and press Enter.

```
securityHardeningOptions selinux,audit,fips,aide,TLSv1.2enable
```

The system takes a few minutes to complete the setting and reboots for the changes to take effect.



---

## Disabling security hardening options

### About this task

Use this procedure to disable one or more security hardening options from the following:

- selinux
- audit
- aide

### Procedure

1. Log in to the System Manager command line interface.
2. Do one of the following:

- To disable only one security hardening option, type `securityHardeningOptions <security_hardening_option_name> disable`, and press Enter.

For example, type the following command, and press Enter.

```
securityHardeningOptions selinux disable
```

- To disable more than one security hardening options, type `securityHardeningOptions <Comma separated_security_hardening_option_name> disable`, and press Enter.

For example, type the following command, and press Enter.

```
securityHardeningOptions selinux,audit,aide disable
```

The system takes a few minutes to complete the setting and reboots for the changes to take effect.

---

## Viewing the status of the security hardening options

### Procedure

1. Log in to the System Manager command line interface.
2. Type the command: `securityHardeningOptions --showstate`.

Based on the system state, the system displays the following message.

```
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28

FIPS State : enabled.
```

```
Audit: enabled
AIDE: enabled
Minimum TLS version = TLSv1.2
SMGR Hardening mode: fips
```

---

## Configuring the TLS cipher suite list

### About this task

With System Manager Release 8.0, the TLS cipher suite lists for establishing a secure communication are:

- Strict cipher suite list
- Relax cipher suite list

When you deploy the System Manager Release 8.0 OVA or upgrade System Manager to Release 8.0, by default, the system enables the Relax cipher suite list.

Use the following procedure to configure the required cipher suite list for the system.

### Procedure

1. Log in to the System Manager command line interface.
2. Do one of the following:
  - To configure strict cipher suite list, type the following command. This would disable CBC ciphers.  
**changeCipherSuiteList LIST2**
  - To configure relax cipher suite list, type the following command. This would enable CBC ciphers.  
**changeCipherSuiteList LIST1**

The system restarts the JBoss service on execution of the cipher suite list command.

---

## Changing the TLS version

---

### Changing the TLS version of System Manager

#### Procedure

1. On the System Manager web console, click **Services > Security**.

2. In the navigation pane, click **Configuration > Security Configuration**.
3. On the Security Configuration page, click **Global**.
4. In the **Minimum TLS Version** field, click the appropriate TLS version.  
For more information, see “Security Configuration field descriptions”.
5. Click **Commit** to save the changes.

---

## Changing the TLS version of primary and secondary System Manager

### About this task

Use the following procedure to change the TLS version of System Manager in the Geographic Redundancy setup.

### Before you begin

Ensure that the system is in the maintenance window.

### Procedure

1. Disable the Geographic Redundancy replication.  
For more information, see “Disabling the Geographic Redundancy replication”.
2. Activate the secondary System Manager server.  
For more information, see “Activating the secondary System Manager server”.
3. On the primary System Manager server, change **Minimum TLS Version**.  
For more information, see “Changing the TLS version of System Manager”.  
Wait until the JBoss service starts. JBoss service automatically restarts after 10 minutes.
4. On the secondary System Manager server, change **Minimum TLS Version**.  
For more information, see “Changing the TLS version of System Manager”.  
Wait until the JBoss service starts. JBoss service automatically restarts after 10 minutes.
5. Deactivate the secondary System Manager server.  
For more information, see “Deactivating the secondary System Manager server”.
6. Restore data on the primary System Manager server and note the following:  
For more information, see “Restoring the primary System Manager server”.
  - a. Perform the **Restore Data** operation from the secondary System Manager server.
  - b. Ensure to select **Primary System Manager**.
7. Enable the Geographic Redundancy replication.  
For more information, see “Enabling the Geographic Redundancy replication”.

**Related links**

[Disabling the Geographic Redundancy replication](#) on page 112  
[Activating the secondary System Manager server](#) on page 113  
[Changing the TLS version of System Manager](#) on page 1168  
[Deactivating the secondary System Manager server](#) on page 114  
[Restoring the primary System Manager server](#) on page 115  
[Enabling the Geographic Redundancy replication](#) on page 111

---

## outboundConnectionLogging command

The **outboundConnectionLogging** command captures the logs in the `/var/log/Avaya/connections` file for every new outgoing connections initiated from System Manager.

By default, the outbound connection logging is disabled.

If you need to monitor logs, you can enable the outbound connection logging. Note that this can generate large amount of logs in the log file and might slightly impact the performance of System Manager. Therefore, it is recommended to disable the outbound connection logging, once your job is complete.

**Syntax**

```
outboundConnectionLogging [enable] [disable]
```

**enable**                Enables the outbound connection logging.

**disable**              Disables the outbound connection logging.

**Related links**

[Enabling outbound connection logging](#) on page 1170  
[Disabling outbound connection logging](#) on page 1171

---

## Enabling outbound connection logging

**Procedure**

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type `outboundConnectionLogging enable`, and press `Enter`.
3. When the system prompts for privileged command execution verification [`sudo`], type the password.

System Manager enables the outbound connection logging.

**Related links**

[outboundConnectionLogging command](#) on page 1170

---

## Disabling outbound connection logging

**Procedure**

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type `outboundConnectionLogging disable`, and press `Enter`.
3. When the system prompts for privileged command execution verification [`sudo`], type the password.

System Manager disables the outbound connection logging.

**Related links**

[outboundConnectionLogging command](#) on page 1170

---

## configureOutboundFirewall command

With Release 8.1.3, you can configure System Manager outbound firewall by using the **configureOutboundFirewall** command.

When you configure the outbound firewall rule, System Manager can connect only to those destination system that are added in the allowed whitelist. Therefore, when you add the very first outbound firewall rule, ensure that you add all the required destination IP Addresses in the allowed whitelist to which System Manager will connect to.

By using the **configureOutboundFirewall** command, you can add, list, view status, disable, remove, and overwrite the IP addresses and FQDN in the whitelist for establishing the outbound connection from System Manager. You can also enable, disable, and view the status of logs for any connection that are dropped. This command supports the IPv4, IPv6, FQDN, and Network with Classless Inter-Domain Routing (CIDR) notation addresses.

Note the following:

- In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.
- By using, the **configureOutboundFirewall** command, you cannot configure the outbound firewall in the Software-only environment.

**Syntax**

```
configureOutboundFirewall [add {-s} {-f}] [list] [status] [remove {-e} {-f}] [disable]
[overwrite {-s} {-f}] [enable-logging] [disable-logging] [logging-status]
```

|                                    |                                                                                                                                                                                                                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-h</b>                          | Displays the help for the command.                                                                                                                                                                                                                                                       |
| <b>add -s</b>                      | Adds the destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist. While processing the FQDN, System Manager resolves the FQDN to its IP Address, and adds that IP address in the whitelist. You can add multiple entries with comma-separated values. |
| <b>add -f</b>                      | Adds the destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist through a file.                                                                                                                                                                      |
| <b>list</b>                        | Displays the list of outbound firewall rules.                                                                                                                                                                                                                                            |
| <b>status</b>                      | Displays the status of outbound firewall configuration.                                                                                                                                                                                                                                  |
| <b>remove -e</b>                   | Removes the entry of the outbound firewall rules from the whitelist.                                                                                                                                                                                                                     |
| <b>remove -f</b>                   | Removes the file of the destination outbound firewall rules.                                                                                                                                                                                                                             |
| <b>disable</b>                     | Disables the outbound firewall rules.                                                                                                                                                                                                                                                    |
| <b>overwrite -s</b>                | Overwrites the existing list of outbound firewall rules in the whitelist.                                                                                                                                                                                                                |
| <b>overwrite -f<br/>INPUT_FILE</b> | Overwrites the existing file of outbound firewall rules.                                                                                                                                                                                                                                 |
| <b>enable-logging</b>              | Captures the logs for any dropped connections. By default, the outbound firewall rule logging is disabled. System Manager stores the logs in the <code>/var/log/outbound_firewall.log</code> file.                                                                                       |
| <b>disable-logging</b>             | Disables the outbound firewall rule logging.                                                                                                                                                                                                                                             |
| <b>logging-status</b>              | Displays the outbound firewall rule logging status.                                                                                                                                                                                                                                      |

#### Related links

[Configuring the outbound firewall rules](#) on page 1173  
[Viewing the list of outbound firewall rules](#) on page 1174  
[Viewing the outbound firewall rule status](#) on page 1174  
[Removing outbound firewall rules](#) on page 1175  
[Disabling the outbound firewall rule](#) on page 1175  
[Overwriting the existing outbound firewall rules](#) on page 1176  
[Managing the outbound firewall rule logging](#) on page 1177

## Configuring the outbound firewall rules

### About this task

When you configure the outbound firewall rule, System Manager can connect only to those destination system that are added in the allowed whitelist. Therefore, when you add the very first outbound firewall rule, ensure that you add all the required destination IP Addresses in the allowed whitelist to which System Manager will connect to.

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:

- To add the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist, type **configureOutboundFirewall add -s** *<destination IPv4/IPv6/FQDN/CIDR IPs>*, and press Enter.

You can add multiple entries with comma-separated values.

For example, to add the specific entries, type the following:

```
configureOutboundFirewall add -s
10.10.10.10,10.10.10.11,test.avaya.com,10.10.10.12/24,2a07:2a42:adc0:19::9:25
```

- To add the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist through a file, type **configureOutboundFirewall add -f** *<absolute path of the.txt file>*, and press Enter.

You can add each entry in a separate line in the *<nameofthefile>.txt* file.

For example, the format of the file is:

```
cat /home/location/filename.txt
10.10.10.10
10.10.10.11
2a07:2a42:adc0:19::9:25
test.avaya.com
10.10.10.12/24
```

For example, to add the entries through the file, type the following:

```
configureOutboundFirewall add -f /home/location/filename.txt
```

While processing the FQDN, System Manager resolves the FQDN to its IP Address, and then adds, removes, or overwrites that IP address in the whitelist.

3. If the system prompts, type *y* to continue.

In the Geographic Redundancy setup, System Manager displays the following message:

Geographic Redundancy configuration detected. Separate configuration of Outbound Firewall is required on the Primary and Secondary servers.

In the Geographic Redundancy setup, if you need to configure the outbound firewall rules, then you need to add the peer IP addresses on the primary and secondary System Manager servers.

System Manager adds the specified IP Addresses and FQDN in the whitelist.

#### Related links

[configureOutboundFirewall command](#) on page 1171

---

## Viewing the list of outbound firewall rules

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type `configureOutboundFirewall list`, and press `Enter`.

System Manager displays the outbound firewall rule status and the list of the outbound firewall rules that are configured.

For example:

```
OutBound connection firewall rules enabled

Following IP Addresses / Networks allowed for OutBound connection

10.10.10.11
10.10.10.12/24

2a07:2a42:adc0:19::9:25
```

#### Related links

[configureOutboundFirewall command](#) on page 1171

---

## Viewing the outbound firewall rule status

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type `configureOutboundFirewall status`, and press `Enter`.

The outbound firewall rule status can be `enabled` or `disable`.

System Manager displays the status of the outbound firewall rule.

For example:

```
enabled
```



**Related links**

[configureOutboundFirewall command](#) on page 1171

---

## Removing outbound firewall rules

**Procedure**

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
  - To remove the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in whitelist, type **configureOutboundFirewall remove -e** *<destination IPv4/IPv6/FQDN/CIDR IPs>*, and press Enter.

For example, to remove the specific entries, type the following:

```
configureOutboundFirewall remove -e 10.10.10.10
```

- To remove the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in whitelist through a file, type **configureOutboundFirewall remove -f** *<absolute path of the.txt file>*, and press Enter.

For example, to remove the entries through the file, type the following:

```
configureOutboundFirewall remove -f /home/location/filename.txt
```

While processing the FQDN, System Manager resolves the FQDN to its IP Address, and then adds, removes, or overwrites that IP address in the whitelist.

System Manager removes the specified IP Addresses, FQDN, and CIDR notation IP addresses from the whitelist.

**Related links**

[configureOutboundFirewall command](#) on page 1171

---

## Disabling the outbound firewall rule

**About this task**

If you disable the outbound firewall rule, System Manager removes all the rules from the whitelist. Later, if you need to enable the outbound firewall rule, then you need to again add all the details in the whitelist.

**Procedure**

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Type **configureOutboundFirewall disable**, and press Enter.

3. At the prompt, type `y` to continue.

System Manager disables the outbound firewall rule.

#### Related links

[configureOutboundFirewall command](#) on page 1171

## Overwriting the existing outbound firewall rules

### About this task

If you overwrite the outbound firewall rule, System Manager removes all the existing rules from the whitelist and adds the new entries in the whitelist.

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
  - To overwrite the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in whitelist, type **configureOutboundFirewall** `overwrite -s` *<destination IPv4/IPv6/FQDN/CIDR IPs>*, and press Enter.

For example, to overwrite the specific entries, type the following:

```
configureOutboundFirewall overwrite -s
10.10.10.14,10.10.10.15,example.avaya.com,10.10.10.16/24,2a07:2a4
2:adc0:19::9:25
```

- To overwrite the list of destination IPv4, IPv6, FQDN, and Network with CIDR notation IP addresses in the whitelist through a file, type **configureOutboundFirewall** `overwrite -f` *<absolute path of the.txt file>*, and press Enter.

You can enter each entry in a separate line in the *<nameofthefile>.txt* file.

For example, the format of the file is:

```
cat /home/location/filename.txt
10.10.10.14
10.10.10.15
2a07:2a42:adc0:19::9:25
example.avaya.com
10.10.10.16/24
```

For example, to overwrite the entries through the file, type the following:

```
configureOutboundFirewall overwrite -f /home/location/
filename.txt
```

While processing the FQDN, System Manager resolves the FQDN to its IP Address, and then adds, removes, or overwrites that IP address in the whitelist.

System Manager overwrites the existing IP Addresses and FQDN with the new details in the whitelist.

#### Related links

[configureOutboundFirewall command](#) on page 1171

---

## Managing the outbound firewall rule logging

### About this task

Use this procedure to enable, disable, or view the status of the outbound firewall rule logging for the dropped connections.

If you need to monitor logs, you can enable the outbound firewall rule logging. Note that this can generate large amount of logs in the log file and might slightly impact the performance of System Manager. Therefore, it is recommended to disable the outbound firewall rule logging, once your job is complete.

### Before you begin

Log in to the System Manager command line interface with CLI user credentials that you created at the time of application deployment.

- To enable the outbound firewall rule logging, type **configureOutboundFirewall enable-logging**, and press **Enter**.

System Manager enables the outbound firewall rule logging and captures the logs for the dropped connections in the `/var/log/outbound_firewall.log` file.

- To disable the outbound firewall rule logging, type **configureOutboundFirewall disable-logging**, and press **Enter**.

By default the outbound firewall rule logging is disabled.

System Manager disables the outbound firewall rule logging and does not captures the logs for the dropped connections.

- To view the outbound firewall rule logging status, type **configureOutboundFirewall logging-status**, and press **Enter**.

System Manager displays the outbound firewall rule logging status.

#### Related links

[configureOutboundFirewall command](#) on page 1171

---

## Managing certificates

---

### Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices for a secure, interelement communication. Trust Management provides Identity (Server) and Trusted (Root/CA) certificates that applications can use to establish mutually authenticated Transport Layer Security (TLS) sessions.

System Manager validates any file that you upload during certificate management, and accepts only certain file types, such as text and XML. System Manager filters uploaded files based on file extension and mime types or bytes in the file.

System Manager uses a third-party open source application, Enterprise Java Beans Certificate Authority (EJBCA), as a Certificate Authority for certificate management.

From Manage Elements, you can manage certificates for System Manager and the elements that System Manager supports.

#### Related links

[Certificate Authorities](#) on page 1209

---

## Certificate generation and certificate management capabilities in System Manager

The table provides the major certificate generation and certificate management capabilities that System Manager offers. System Manager manages certificates for System Manager and elements that System Manager manages.

All communications between the client and the servers in the Avaya Aura® environment are secured using the Transport Layer Security (TLS) protocol. In TLS, servers are configured with an identity certificate issued by a certificate authority. When clients connect to servers, the server presents its identity certificate for the client to validate. The client checks whether the server identity certificate was issued by a certificate authority that the client trusts. If the validation succeeds, a secure connection is established.

| # | Use case                                                                                                                                                              | Example                                                                                                                                                                                                                                                                                                                              | With System Manager CA as Root CA<br>Default mode | With System Manager CA as SubCA | With third-party CA signed identity certificates |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|---------------------------------|--------------------------------------------------|
| 1 | New certificate generation by using the SCEP client                                                                                                                   | <ul style="list-style-type: none"> <li>Request from a product that is integrated with System Manager for certificates during installation. For example, Session Manager.</li> <li>Request for certificates during the installation or registration of devices or endpoints that hosts an SCEP client. For example, B5800.</li> </ul> | ✓                                                 | ✓                               | Not applicable                                   |
| 2 | New certificate generation by System Manager by using: <ul style="list-style-type: none"> <li>Standard Certificate Signing Request (CSR)</li> <li>Keystore</li> </ul> | Generating certificates manually to install the certificates on remote instances of: <ul style="list-style-type: none"> <li>Various products or endpoints</li> <li>Products that want to generate the keys on product and require System Manager CA to sign the certificates.</li> </ul>                                             | ✓                                                 | ✓                               | Not applicable                                   |

Table continues...

| # | Use case                                                                                                                 | Example                                                                                                                                                                                                                                                                        | With System Manager CA as Root CA<br>Default mode | With System Manager CA as SubCA | With third-party CA signed identity certificates |
|---|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|---------------------------------|--------------------------------------------------|
| 3 | Installing a new identity certificate issued by a third-party CA                                                         | Configuring the System Manager web interface to use a certificate issued by a well-known CA, for example, VeriSign, instead of a certificate issued by own CA. This applies for products that use System Manager for administration. For example, Session Manager and CS 1000. | ✓                                                 | ✓                               | ✓                                                |
| 4 | Replacing an identity certificate issued by the System Manager CA with a new certificate issued by System Manager CA     | Installing a new certificate with changed values. For example, new FQDN and new IP address.                                                                                                                                                                                    | ✓                                                 | ✓                               | Not applicable                                   |
| 5 | Replacing an existing identity certificate issued by a third-party CA with a new certificate issued by System Manager CA | Reverting System Manager, Session Manager, and CS 1000 that use third-party identity certificates to use certificates issued by the System Manager CA.                                                                                                                         | ✓                                                 | ✓                               | ✓                                                |
| 6 | Renewal of an existing identity certificate                                                                              | Manual or automatic renewing of a certificate that is about to expire. This capability is also available for products such as Session Manager.                                                                                                                                 | ✓                                                 | ✓                               | X                                                |

Table continues...

| # | Use case                                                          | Example                                                                                                                                                     | With System Manager CA as Root CA<br>Default mode | With System Manager CA as SubCA | With third-party CA signed identity certificates |
|---|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|---------------------------------|--------------------------------------------------|
| 7 | Exporting an identity certificate to a PEM certificate file       | Exporting any identity certificate to a standard PEM format files so that the certificate can be manually imported to the trust stores of various products. | ✓                                                 | ✓                               | ✓                                                |
| 8 | Adding new certificates to the truststore of the product.         | Installing a new certificate to the truststores of the product, such as Session Manager.                                                                    | ✓                                                 | ✓                               | ✓                                                |
| 9 | Removing existing certificates from the truststore of the product | Deleting a certificate, for example, SIPCA root certificate, from the truststores of the product such as Session Manager.                                   | ✓                                                 | ✓                               | ✓                                                |

The certificate that is used to assert its identity is called a product certificate or an identity certificate. The issuer or CA certificate used to verify and validate the identity of the far end is referred to as the trusted certificate or CA certificate.

## Setting the enrollment password

### About this task

You can use this functionality to generate the enrollment password for managed elements. The managed elements require the enrollment password to request certificates from System Manager Trust Management.

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Enrollment Password**.

3. On the Enrollment Password page, in the **Password expires in** field, select a password expiration time in hours, days, or weeks.

The screenshot shows the 'Enrollment Password' page in the Avaya Aura System Manager. The left sidebar contains a 'Security' menu with options like Certificates, Authority, Enrollment Password, Manage Certificate, Revocation, and Configuration. The main content area has a breadcrumb trail 'Home / Services / Security / Certificates / Enrollment Password'. The page title is 'Enrollment Password'. Below the title, there is a message 'Need to set a valid enrollment password.' and a 'Time Remaining' section showing '00 hour 00 mins'. The 'New Password' section includes three fields: 'Password expires in' (a dropdown menu), 'Password' (a text input field), and 'Confirm Password' (a text input field). A 'Commit' button is located at the bottom right of the form.

4. In **Password** and **Confirm Password** fields, enter the password.
5. Click **Commit**.

The system updates the time displayed in the Time remaining section with the value that you selected in **Password expires in**.

6. Note the password for future reference.

The Authority link is used for launching EJBCA administration. A customer can configure the settings here, based on its PKI plan.

The screenshot shows the 'CA Structure & CRLs' page in the Avaya Aura System Manager. The left sidebar contains a 'CA Functions' menu with options like CA Activation, CA Structure & CRLs, Certificate Profiles, Certification Authorities, Crypto Tokens, Publishers, RA Functions, Add End Entity, End Entity Profiles, Search End Entities, User Data Sources, Supervision Functions, Approve Actions, and View Log. The main content area has a title 'CA Structure & CRLs'. Below the title, there is a section 'Basic Functions for CA : tmdefaultca' with links 'View Certificate' and 'View Information'. The 'Root CA' section shows 'CN=System Manager CA,OU=MGMT,O=AVAYA' and links 'Download binary/to IE', 'Download to Firefox', 'Download PEM file', and 'Download BCFKS file'. The 'Latest CRL' section shows 'Created 2017-02-09 12:59:42+05:30, Expires 2017-02-16 12:59:42+05:30, number 3' and a link 'Get CRL'. The 'Delta CRLs' section shows 'Delta CRLs are not enabled.' and a 'Create a new updated CRL' button with a 'Create CRL' button. At the bottom, there is a footer 'Made by PrimeKey Solutions AB, 2002–2014.'



### Related links

[Enrollment Password field descriptions](#) on page 1183

## Enrollment Password field descriptions

| Name                       | Description                                                                     |
|----------------------------|---------------------------------------------------------------------------------|
| <b>Time Remaining</b>      | The time in hours and minutes remaining for expiration of the current password. |
| <b>Password expires in</b> | The duration in hours for which the existing password is valid.                 |
| <b>Password</b>            | The password that the external clients use to request for a certificate.        |
| <b>Confirm Password</b>    | The password that you retype.                                                   |

| Button        | Description                                                            |
|---------------|------------------------------------------------------------------------|
| <b>Commit</b> | Updates the <b>Existing Password</b> and <b>Time Remaining</b> fields. |

## Managing trusted certificates

### Obtaining the SSL certificate for Microsoft Active Directory

#### Procedure

1. Install the certification authority (CA) on your Microsoft Active Directory server. For information, see <https://support.microsoft.com/en-us>.
2. Run the following command on the Microsoft Active Directory server to export the certificate:

```
certutil -ca.cert client.crt
```

3. Copy the `client.crt` file from the Microsoft Active Directory server to your computer.

## Next steps

Import the certificate for Microsoft Active Directory server to System Manager.

For instructions, see Adding trusted certificates.

## Related links

[Adding trusted certificates](#) on page 1184

## Adding trusted certificates

### About this task

From Release 8.1, you can add trusted certificates for multiple elements. All the elements must be of same ElementType and Version. When you add trusted certificates for multiple elements of same ElementType and Version, the system creates a job. You can view the certificate management job status by clicking **View Certificate Add Status** on the Manage Elements page.

The flow for adding a trusted certificate for single element is the same. The system does not create a job for adding trusted certificate for single element.

Use the following procedure to import the certificates that you want to add as trusted certificate in the trust store of the element.

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select one or more element, and click **More Actions > Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.

#### Manage Trusted Certificates

[View](#) [Add](#) [Export](#) [Remove](#)

| 10 Items  |                                                      |                           | Filter: Enable                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------|------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/>                                                                     | Store Description                                    | Store Type                | Subject Name                                                                                                                                                                                   |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | USER_CERT_BASED_LOGIN_TLS | O=AVAYA, OU=MGMT, CN=System Manager CA                                                                                                                                                         |
| <input type="checkbox"/>                                                                     | Used for validating TLS server identity certificates | TM_OUTBOUND_TLS           | O=AVAYA, OU=MGMT, CN=System Manager CA                                                                                                                                                         |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS_PEM        | O=AVAYA, OU=MGMT, CN=System Manager CA                                                                                                                                                         |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | CN=ESDP CA, OU=Avaya Global Services, OU=Class 2 Managed PKI Individual Subscriber CA, OU=Terms of use at https://www.verisign.com/rpa (c)06, OU=VeriSign Trust Network, O="Avaya, Inc.", C=US |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | CN=Avaya File Signing Authority 2013, OU=Avaya Product PKI, O=Avaya Inc., C=US                                                                                                                 |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US                   |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | CN=Avaya File Signing Authority 2013, OU=Avaya Product PKI, O=Avaya Inc., C=US                                                                                                                 |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | CN=VeriSign Class 3 Secure Server CA - G3, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US                                          |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | O=AVAYA, OU=MGMT, CN=System Manager CA                                                                                                                                                         |
| <input type="checkbox"/>                                                                     | Used for validating TLS client identity certificates | TM_INBOUND_TLS            | CN=Avaya Client Services Users CA, OU=Avaya IT, OU=Class 2 Managed PKI Individual Subscriber CA, OU=Symantec Trust Network, O="Avaya, Inc.", C=US                                              |

Select : All, None

4. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select a store type or select **All** if you are unsure of the store type.
5. To import certificates from a file, do the following:
  - a. Click **Import from file**.

- b. Type the file name or click **Browse** to select a file.

 **Note:**

System Manager validates the file type. If you provide an invalid file type, the system displays an error message.

- c. Click **Retrieve Certificate**.
6. To import certificates in the PEM format, do the following:
  - a. Locate the PEM certificate.
  - b. Open the certificate in the Notepad application.
  - c. Select and copy the contents in the file.
  - d. On the Add Trusted Certificates page, click **Import as PEM certificate**.
  - e. Paste the contents from the PEM file in the text box provided on the Add Trusted Certificates page.
7. To import certificates from existing certificates, do the following:
  - a. Click **Import from existing certificates**.
  - b. In the Global Trusted Certificate section, select a certificate.
8. To import certificates by using TLS, do the following:
  - a. Click **Import using TLS**.
  - b. In **IP Address**, type the IP address of the computer.
  - c. In **Port**, type the port of the computer.
  - d. Click **Retrieve Certificate**.
9. Click **Commit**.
10. Restart the JBoss service on System Manager.

#### Related links

[Add Trusted Certificate field descriptions](#) on page 1185

[Obtaining the SSL certificate for Microsoft Active Directory](#) on page 1183

#### Add Trusted Certificate field descriptions

| Name                                                | Description                                                                                                                                                                     |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Store Type to add trusted certificate</b> | The store type that is based on inbound and outbound connection.                                                                                                                |
| <b>Import from file</b>                             | The option to import a certificate from a file. The file format is <code>.cer</code> or <code>.crt</code> .                                                                     |
| <b>Import as PEM certificate</b>                    | The option to import a certificate in the PEM format. When you select <b>Import as PEM certificate</b> , the system displays the text box to paste the PEM certificate content. |

*Table continues...*

| Name                                     | Description                                                                                                               |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Import from existing certificates</b> | The option to import a certificate from the existing imported certificates.                                               |
| <b>Import using TLS</b>                  | The option to import a certificate if the element requires to contact the certificate provider to obtain the certificate. |

When you select **Import from file**, the page displays the following fields.

| Name                        | Description                              |
|-----------------------------|------------------------------------------|
| <b>Please select a file</b> | The file that contains the certificates. |

| Button                      | Description                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Browse</b>               | Displays the choose file dialog box where you can choose the file from which you want to import the certificates.        |
| <b>Retrieve Certificate</b> | Retrieves the certificate from the file, and displays the details of the certificate in the Certificate Details section. |

### Certificate Details:

The page displays these fields when you click **Retrieve**.

| Name                           | Description                                                                                                                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject Details</b>         | The details of the certificate holder.                                                                                                                                                            |
| <b>Valid From</b>              | The date and time from when the certificate is valid.                                                                                                                                             |
| <b>Valid To</b>                | The date and time until when the certificate is valid.                                                                                                                                            |
| <b>Key Size</b>                | The size of the key in bits for encryption.                                                                                                                                                       |
| <b>Issuer Name</b>             | The name of the issuer of the certificate.                                                                                                                                                        |
| <b>Certificate Fingerprint</b> | The fingerprint that authenticates the entire certificate.                                                                                                                                        |
| <b>Key Fingerprint</b>         | The fingerprint that authenticates the key. The Key fingerprint applies only for CA certificate. Therefore, any element, which calculates fingerprint using the key, can use this authentication. |
| <b>CA Certificate</b>          | The field that specifies whether the certificate is a CA certificate.                                                                                                                             |

### Global Trusted Certificate:

When you select **Import from existing certificates**, the page displays the following fields.

| Name                    | Description                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------|
| <b>Certificate Name</b> | The fully qualified domain name of the certificate.                                               |
| <b>Subject Name</b>     | The fully qualified domain name of the certificate holder.                                        |
| <b>Valid To</b>         | The date until which the certificate is valid.                                                    |
| <b>Filter: Enable</b>   | Displays fields in select columns where you can set the filter criteria. This is a toggle button. |

*Table continues...*

| Name                   | Description                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------|
| <b>Filter: Disable</b> | Hides the column filter fields without resetting the filter criteria. This is a toggle button. |
| <b>Filter: Clear</b>   | Clears the filter criteria.                                                                    |
| <b>Filter: Apply</b>   | Filters certificates based on the filter criteria.                                             |
| <b>Select: All</b>     | Selects all the certificates in the table.                                                     |
| <b>Select: None</b>    | Clears all the check box selections.                                                           |
| <b>Refresh</b>         | Refreshes the certificates information.                                                        |

The page displays these fields when you select the **Import using TLS** option.

| Name              | Description                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------|
| <b>IP Address</b> | The IP address of the certificate provider that is to be contacted for retrieving the certificate. |
| <b>Port</b>       | The port of the server to be used for obtaining the certificate.                                   |

| Button                      | Description                                                                                               |
|-----------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Retrieve Certificate</b> | Retrieves the certificate and displays the details of the certificate in the Certificate Details section. |

#### Related links

[Adding trusted certificates](#) on page 1184

## Viewing trusted certificates

### About this task

You can view the trusted certificates of System Manager and its managed elements.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions > Manage Trusted Certificates**.
4. On the Manage Trusted Certificates page, select the required certificate and click **View**.

The View Trust Certificate page displays the details of the selected certificate.

#### Related links

[View Trust Certificate field descriptions](#) on page 1188

## View Trust Certificate field descriptions

| Name                           | Description                                                                                                                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject Details</b>         | The details of the certificate holder.                                                                                                                                                            |
| <b>Valid From</b>              | The date and time from which the certificate is valid.                                                                                                                                            |
| <b>Valid To</b>                | The date and time until which the certificate is valid.                                                                                                                                           |
| <b>Key Size</b>                | The size of the key in bits for encryption.                                                                                                                                                       |
| <b>Issuer Name</b>             | The name of the issuer of the certificate.                                                                                                                                                        |
| <b>Certificate Fingerprint</b> | The fingerprint that authenticates the entire certificate.                                                                                                                                        |
| <b>Key Fingerprint</b>         | The fingerprint that authenticates the key. The Key fingerprint applies only for CA certificate. Therefore, any element, which calculates fingerprint using the key, can use this authentication. |
| <b>Serial Number</b>           | The serial number of the certificate.                                                                                                                                                             |
| <b>Basic Constraints</b>       | The extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.                                         |
| <b>Key Usage Extension</b>     | The extension defines the purpose of the key contained in the certificate such as Digital Signature, Key Cert Sign, CRL Sign.                                                                     |
| <b>Extended Key Usage</b>      | This extension indicates one or more purposes for which the certified public key may be used. in addition to or in place of the basic purposes indicated in the key usage extension.              |

| Button      | Description                                                   |
|-------------|---------------------------------------------------------------|
| <b>Done</b> | Closes the page and returns to the Trusted Certificates page. |

## Removing trusted certificates

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an application and click **More Actions > Manage Trusted Certificates**.
4. On the Manage Trusted Certificates page, select the certificates you want to remove.
5. Click **Remove**.

Trust Management removes the certificates from the list of trusted certificates for the application you selected.

## Delete Trusted Certificate Confirmation field descriptions

Use this page to delete a trusted certificate from the list of trusted certificate maintained by the element.

| Field                   | Description                                            |
|-------------------------|--------------------------------------------------------|
| <b>Certificate Name</b> | The common name of the certificate.                    |
| <b>Store Type</b>       | The type of the store associated with the certificate. |
| <b>Subject Name</b>     | The name of the certificate holder.                    |

| Button        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| <b>Delete</b> | Deletes the trusted certificate from the corresponding store.                 |
| <b>Cancel</b> | Cancels the delete operation and returns to the Add Trusted Certificate page. |

## Trusted certificate management

Participants in a Public-Key Infrastructure (PKI) scheme use root certification authorities and other intermediate certification authorities to determine the trustworthiness of an identity certificate. These certification authorities are collectively known as trust anchors or trusted certificates.

System Manager certificate management supports the following tasks on the trusted certificate of a service:

- **View:** Trust Management provides details about the subject, issuer, key size, fingerprint, and expiry date of the certificate that a service uses.
- **Add:** A service may require to communicate with another service outside the deployment PKI of Avaya Aura®. For example, for a service to gain access to a remote database or a directory service which presents an identity certificate signed by a commercial CA, include the certificate of the CA in the list of trusted certificates of the service.

For example, if a service is exposed to multiple SIP endpoints, you cannot add the certificate of the private Certificate Authority (CA) to the trusted certificate store of each client. If each SIP endpoint is configured to trust certificates issued by a commercial CA, replace the certificate presented by the endpoint with a certificate of the commercial CA or the root certificate of the commercial CA. You can add a certificate to a trusted certificate store of the service in the following encodings:

- ASN.1 DER
- PEM (OpenSSL)

You can also get a certificate from an SSL socket or from the built-in certificate store.

- **Export:** Trust Management supports exporting the selected certificate from the list of trusted certificates to a PEM formatted file.
- **Delete:** When you do not need a service to participate in an external PKI hierarchy, the administrator can remove the trusted certificate from the trusted certificate store of the service. For example, when CA changes, you do not require the existing CA.

### Manage Trusted Certificates field descriptions

Use this page to view, export, and remove the trusted certificates listed on the page. You can add more certificates in the existing list of trusted certificates.

| Name                     | Description                                            |
|--------------------------|--------------------------------------------------------|
| <b>Store Description</b> | The purpose of the trusted certificate.                |
| <b>Store Type</b>        | The type of the store associated with the certificate. |
| <b>Subject Name</b>      | The name of the certificate holder.                    |

| Button        | Description                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------|
| <b>View</b>   | Displays the View Trust Certificate page. Use this page to view the certificate details.                    |
| <b>Add</b>    | Displays the Add Trusted Certificate page. Use this page to import certificates from the selected resource. |
| <b>Export</b> | Exports the selected certificate from the list of trusted certificates to a PEM formatted file.             |
| <b>Remove</b> | Removes the selected certificate from the list of trusted certificates.                                     |

## Managing identity certificates

### Adding additional certificate for a service

#### About this task

Use this procedure to add an additional certificate for following services:

- securitymodule\_http (HTTP)
- securitymodule\_sip (SIP)

#### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select an element, and click **More Actions > Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select the service name to which you want to add another certificate.
4. Click **Add**.

The system displays the Add Identity Certificate page.

5. Click **Add new internal CA signed certificate**, and do the following:
  - a. Select the **Common Name (CN)** check box and type the common name that is defined in the existing certificate.
  - b. In **Key Algorithm**, select the key algorithm.  
System Manager uses the SHA2 algorithm for generating certificates.
  - c. In **Key Size**, select the required key size.
  - d. In **Subject Alternative Name**, select the relevant options, and enter the details.



- e. **(Optional)** In **OtherName**, type the other name for the certificate signing request.
  - f. To add the internal CA signed certificate, click **Commit**.
6. Click **Add new external CA signed certificate**, and do the following:
  - a. In **Please select a file (PKCS#12 format)**, choose the file from your local computer.
  - b. In **Password**, type the password.
  - c. Click **Retrieve Certificate**.  
 The Certificate Details section displays the details of the certificate.
  - d. Review the details of the uploaded certificate.
  - e. To add a new, external CA-signed certificate, click **Commit**.
7. Click **Generate Certificate Signing Request (CSR) for adding external CA signed certificate**, and do the following:
  - a. Select the **Common Name (CN)** check box and type the common name that is defined in the existing certificate.
  - b. In **Key Algorithm**, select the key algorithm.  
 System Manager uses the SHA2 algorithm for generating certificates.
  - c. In **Key Size**, select the required key size.
  - d. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.
  - e. In **OtherName**, type the other name for the certificate signing request.
  - f. Click **Generate CSR**.
  - g. Ensure that the downloaded CSR is third-party signed.
  - h. Import the signed certificate by using the **Import third party certificate** option.
8. For the newly generated certificates to take effect, restart JBoss on System Manager.

## Making a certificate as a default certificate for a service

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select an element, and click **More Actions > Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select the service name.
4. Click the **Expand List** icon and select an additional certificate.
5. Click **Make default**.

The system displays the following message: Do you want to make this certificate as default certificate for Service Name: <ServiceName>?

6. Click **OK**.

## Removing an additional identity certificate

### About this task

Use this procedure to remove the additional certificate for a service. You cannot remove the default certificate of a service.

### Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. On the Manage Elements page, select an element, and click **More Actions > Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select the service name.
4. Click the **Expand List** icon and select the additional certificate.
5. Click **Remove**.

The system displays the following message: Do you want to delete this certificate of Service Name: <ServiceName>?

6. Click **OK**.

## Viewing identity certificates

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element, and click **More Actions > Manage Identity Certificates**.

The Identity Certificate page displays the identity certificates for the element that you selected. The certificate signed by the Avaya CA is the default.

### Related links

[Identity Certificates field descriptions](#) on page 1195

## Replacing an identity certificate

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions > Manage Identity Certificates**.
4. On the Manage Identity Certificates page, select the certificate that you want to replace.
5. Click **Replace**.

The system displays the Replace Identity Certificate page.

6. Click **Replace this Certificate with Internal CA Signed Certificate**, and do the following:
  - a. Select the **Common Name (CN)** check box and type the common name that is defined in the existing certificate.
  - b. Select the key algorithm and key size from the respective fields.  
System Manager uses the SHA2 algorithm for generating certificates.
  - c. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.
  - d. **(Optional)** In **OtherName**, type the other name for the certificate signing request.
  - e. To replace the identity certificate with the internal CA signed certificate, click **Commit**.
7. Click **Import third party certificate**, and do the following:
  - a. In the **Please select a file** field, choose the file from your local computer.
  - b. In the **Password** field, type the password.
  - c. Click **Retrieve Certificate**.  
The Certificate Details section displays the details of the certificate.
  - d. Review the details of the uploaded certificate.
  - e. To replace the certificate with the third-party certificate that you imported, click **Commit**.
8. Click **Generate Certificate Signing Request (CSR) for third party certificate**, and do the following:
  - a. Select the common name (CN) check box and type the common name that is defined in the existing certificate.
  - b. Select the key algorithm and key size from the respective fields.  
System Manager uses the SHA2 algorithm for generating certificates.
  - c. **(Optional)** In **Subject Alternative Name**, select the relevant options and enter the details.
  - d. In **OtherName**, type the other name for the certificate signing request.
  - e. Click **Generate CSR**.
  - f. Ensure that the downloaded CSR is third-party signed.
  - g. Import the signed certificate using the **Import third party certificate** option.
9. For the newly generated certificates to take effect, restart JBoss on System Manager.

#### Related links

[Replace Identity Certificate field descriptions](#) on page 1195

## Renewing identity certificates

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. On the Manage Elements page, select an element and click **More Actions > Manage Identity Certificates**.
4. On the Identity Certificates page, select the certificate that you want to renew.
5. Click **Renew**.

Wait until the system renews the certificate.

6. Restart the service for which you renewed the certificate.
7. For the new certificates to take effect, restart JBoss on System Manager.

You must also restart JBoss on System Manager if certificates are auto renewed.

## Identity certificate management

In Public-Key Infrastructure (PKI), an identity certificate is an electronic document, which uses a digital signature to bind a public key with an identity information such as the name of a person or an organization and address of a person or an organization. The identity certificate is also known as digital certificate or public key certificate. You can use the certificate to verify if a public key belongs to a service.

System Manager supports the following tasks on the identity certificate of a service:

- **View:** Trust Management provides details about the subject, issuer, key size, fingerprint, and expiry date of the certificate that a service uses.

Additionally, Trust Management provides subject alternative name.

- **Replace:** Services that are exposed to external clients may require to present an identity certificate issued by a commercial root CA.

For example, if a service is exposed to multiple SIP endpoints, you cannot add the certificate of the private Certificate Authority (CA) to the trusted certificate store of each client. If each SIP endpoint is configured to trust certificates issued by a commercial CA, then replace the certificate presented by the service with a certificate issued by a commercial CA. Also, in protocols like HTTP, the CN value of the certificate must match the host name of the server presenting the certificate. If the host name changes, the CN must change.

- **Export:** Trust Management supports exporting the selected certificate from the list of trusted certificates to a PEM formatted file.
- **Renew:** Central administrator might need to reissue an identity certificate that was originally issued by the deployment CA. For example, an identity certificate has a validity date. Therefore, the administrator must replace the certificate before the certificate expires to avoid rejection of the certificate by the service peer.

## Identity Certificates field descriptions

| Name                       | Description                                                 |
|----------------------------|-------------------------------------------------------------|
| <b>Service Name</b>        | The name of the service that uses the identity certificate. |
| <b>Common Name</b>         | The common name to identify the service.                    |
| <b>Valid To</b>            | The date until which the certificate is valid.              |
| <b>Expired</b>             | Specifies whether the certificate is expired.               |
| <b>Service Description</b> | A brief description about the service.                      |

| Button         | Description                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replace</b> | Displays the Replace Identity Certificate page. Use this page to replace a selected identity certificate with a new certificate.    |
| <b>Export</b>  | Exports the certificate that you select. The exported certificate is in the form of a PEM file.                                     |
| <b>Renew</b>   | Renews the certificate that you select. After you renew a certificate, the system automatically updates the <b>Valid To</b> column. |

## Replace Identity Certificate field descriptions

### Certificate Details

| Name                            | Description                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject Details</b>          | The certificate holder details.                                                                                                                                                                    |
| <b>Valid From</b>               | The date and time from when the certificate is valid.                                                                                                                                              |
| <b>Valid To</b>                 | The date and time till the certificate is valid.                                                                                                                                                   |
| <b>Key Size</b>                 | The key size in bits for encryption. The default key size is 2048.                                                                                                                                 |
| <b>Issuer Name</b>              | The name of the certificate issuer.                                                                                                                                                                |
| <b>Certificate Fingerprint</b>  | The fingerprint that authenticates the certificate.                                                                                                                                                |
| <b>Subject Alternative Name</b> | An alternative name of the certificate holder.                                                                                                                                                     |
| <b>Serial Number</b>            | The serial number of the certificate.                                                                                                                                                              |
| <b>Basic Constraints</b>        | The extension that identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.                                     |
| <b>Key Usage Extension</b>      | The extension that defines the purpose of the key contained in the certificate. For example, Digital Signature, Content Commitment, Key Encipherment, Data Encipherment, and Key Agreement.        |
| <b>Extended Key Usage</b>       | The extension that indicates one or more purposes for which the certified public key can be used. These are in addition to or in place of the basic purposes indicated in the key usage extension. |

| Name                                                                          | Description                                                                                                        |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Replace this Certificate with Internal CA Signed Certificate</b>           | The option to replace the current certificate with the internal CA signed certificate.                             |
| <b>Import third party certificate</b>                                         | The option to replace the identity certificate with the PKCS #12 file that you imported from a third-party source. |
| <b>Generate Certificate Signing Request (CSR) for third party certificate</b> | The option to generate a certificate signing request for a third-party certificate.                                |

When you select **Replace this Certificate with Internal CA Signed Certificate** or **Generate Certificate Signing Request (CSR) for third party certificate**, the system displays the following fields.

| Name                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Common Name (CN)</b>         | The common name of the certificate holder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Key Algorithm</b>            | The algorithm used to generate the key for the certificate.<br>The option is RSA.<br>System Manager uses the SHA2 hash algorithm for generating certificates.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Key Size</b>                 | The key size in bits for encryption. The options are: <ul style="list-style-type: none"> <li>• <b>1028</b></li> <li>• <b>2048</b></li> <li>• <b>4096</b></li> </ul> Use 2048 as the key size.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Subject Alternative Name</b> | An alternative name of the certificate holder. The options are: <ul style="list-style-type: none"> <li>• <b>DNS Name:</b> The DNS IP address.</li> <li>• <b>IP Address:</b> The IP address.</li> <li>• <b>URI:</b> The URI address.</li> </ul> <p> <b>Note:</b></p> <p>In <b>DNS Name</b>, <b>IP Address</b>, and <b>URI</b> fields, you can enter more than one value separated by a comma.</p> <p>Do not add spaces between comma-separated IP addresses and DNS names.</p> |
| Button                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Commit</b>                   | Replaces the current identity certificate with the selected certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Button              | Description                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generate CSR</b> | Generates a third-party certificate signing request.<br><br>When you select the <b>Generate Certificate Signing Request (CSR) for third party certificate</b> option, the system enables the <b>Generate CSR</b> button. |
| <b>Cancel</b>       | Cancels the certificate replacement operation.                                                                                                                                                                           |

When you select **Import third party certificate**, the system displays the following fields.

| Name                                          | Description                                                         |
|-----------------------------------------------|---------------------------------------------------------------------|
| <b>Please select a file (PKCS #12 format)</b> | The full path of the PKCS #12 file where you saved the certificate. |
| <b>Password</b>                               | The password to retrieve the certificate.                           |

| Button                      | Description                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Retrieve Certificate</b> | Retrieves the details of the imported certificate and displays them in the Certificate Details section. |
| <b>Commit</b>               | Replaces the current identity certificate with the selected certificate.                                |
| <b>Cancel</b>               | Cancels the certificate replacement operation.                                                          |

#### Related links

[Replacing an identity certificate](#) on page 1192

## Certificate Revocation

### Viewing the certificates

#### About this task

Use this procedure to view the certificates for managed elements. The managed elements require the certificates to establish connection from System Manager.

#### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Manage Certificate Revocation**.
3. On the Manage Certificate Revocation page, select the certificate that you want to view.
4. Click **View Certificate**.

The system displays the View Certificate Detail page with details of the selected certificate.

5. Click **Done** to close the page.

## View Certificate Detail field descriptions

| Name                     | Description                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Username</b>          | The name of the certificate holder.                                                                               |
| <b>Serial Number</b>     | The serial number that identifies the certificate.                                                                |
| <b>Issuer DN</b>         | The distinguishing name of the certificate issuer.                                                                |
| <b>Subject DN</b>        | The distinguishing name of the certificate holder.                                                                |
| <b>Subject Alt Name</b>  | The alternate name of the certificate holder.                                                                     |
| <b>Revoked</b>           | The option to indicate whether a certificate is revoked.                                                          |
| <b>Revocation Date</b>   | The date when the certificate was revoked.<br>The field remains blank if the certificate is not in revoked state. |
| <b>Revocation Reason</b> | The reason for certificate revocation.<br>The field remains blank if the certificate is not in revoked state.     |
| <b>Valid From</b>        | The date and time from when the certificate is valid.                                                             |
| <b>Valid To</b>          | The date and time till the certificate is valid.                                                                  |
| Button                   | Description                                                                                                       |
| <b>Done</b>              | Closes the View Certificate Detail page and displays the Manage Certificate Revocation page.                      |

## Manage Certificate Revocation field descriptions

| Name                       | Description                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Select radio button</b> | The option to select a certificate.                                                                               |
| <b>Serial Number</b>       | The serial number that identifies the certificate.                                                                |
| <b>Issuer DN</b>           | The distinguishing name of the certificate issuer.                                                                |
| <b>Valid From</b>          | The date and time from when the certificate is valid.                                                             |
| <b>Valid To</b>            | The date and time till the certificate is valid.                                                                  |
| <b>Subject DN</b>          | The distinguishing name of the certificate holder.                                                                |
| <b>Revoked</b>             | The option to indicate whether a certificate is revoked.                                                          |
| <b>Last Updated By</b>     | The name of the user who last updated or edited the certificate or both.                                          |
| <b>Revocation Date</b>     | The date when the certificate was revoked.<br>The field remains blank if the certificate is not in revoked state. |
| <b>Revocation Reason</b>   | The reason for certificate revocation.<br>The field remains blank if the certificate is not in revoked state.     |
| Button                     | Description                                                                                                       |
| <b>View Certificate</b>    | Displays all details of the selected certificate.                                                                 |

*Table continues...*



| Button                      | Description                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------|
| <b>Revoke Certificate</b>   | Displays the option to revoke the selected certificate.                                                    |
| <b>Unrevoke Certificate</b> | Displays the option to unrevoke the selected certificate.                                                  |
| <b>Refresh</b>              | Refreshes the certificate information in the table.                                                        |
| <b>Filter: Enable</b>       | Displays the fields under select columns that you can use to set filter criteria. This is a toggle button. |
| <b>Filter: Disable</b>      | Hides the column filter fields without resetting the filter criteria. This is a toggle button.             |
| <b>Filter: Clear</b>        | Clears the filter criteria.                                                                                |
| <b>Filter: Apply</b>        | Filters certificates based on the filter criteria.                                                         |
| <b>Select: None</b>         | Clears the selections.                                                                                     |
| <b>Previous</b>             | Displays the certificates in the previous page. This button is unavailable when you are on the first page. |
| <b>Next</b>                 | Displays the certificates in the next page. This button is unavailable when you are on the last page.      |

## Revoking and unrevoking certificates

### About this task

Use this procedure to revoke a certificate for applications that System Manager manages. The applications require the certificates to establish connection from System Manager.

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Manage Certificate Revocation**.
3. On the Manage Certificate Revocation page, select a certificate.
4. To revoke the certificate, do the following:
  - a. Ensure that the certificate is in an unrevoked state and click **Revoke**.
  - b. On the Revoke Certificate page, select the reason for certificate revocation.
  - c. Click **Revoke**.
5. To unrevoke the certificate, do the following:
  - a. Ensure that the certificate is in a revoked state with the reason **Certificate hold**.
  - b. Click **Unrevoke**, and on the Revoke Certificate dialog box, click **Ok**.

## Revoke Certificate field descriptions

| Name                 | Description                                        |
|----------------------|----------------------------------------------------|
| <b>Serial Number</b> | The serial number that identifies the certificate. |
| <b>Subject DN</b>    | The distinguishing name of the certificate holder. |

*Table continues...*

| Name                     | Description                                           |
|--------------------------|-------------------------------------------------------|
| <b>Valid From</b>        | The date and time from when the certificate is valid. |
| <b>Valid To</b>          | The date and time till the certificate is valid.      |
| <b>Revocation Reason</b> | The reason to revoke the certificate.                 |

| Button        | Description                                                                             |
|---------------|-----------------------------------------------------------------------------------------|
| <b>Revoke</b> | Saves the certificate revocation reason and revokes the certificate.                    |
| <b>Cancel</b> | Cancels the certificate revocation and displays the Manage Certificate Revocation page. |

## Manage Entity Classes

In Certificate Management, entity classes provide a way to manage certificate issue and renewal for a class (group) of entities with common characteristics, for example Endpoints.

From System Manager Release 8.1.3, you can add, edit, and delete the entity classes by using the **Services > Security > Certificates > Manage Entity Classes** page. Endpoints that have certificates issued by System Manager can use these entity classes to send certificate enrollment or renewal request to System Manager. The entity class password set is used to authenticate enrollment requests from endpoints to System Manager.

## Adding an entity class

### Procedure

1. On the System Manager web console, click **Services > Security > Certificates > Manage Entity Classes**.
2. Click **New**.
3. On the Add Entity Class page, do the following:
  - a. In **Name**, type the name of the entity class.  
The name is mandatory for each entity class.
  - b. In **Description**, type the description of the entity class.
  - c. To enable the white list of subject names associated with an entity class, select the **Whitelist Validation of Subject** check box.
  - d. In **Password**, type the password for the entity class.
  - e. In **Confirm Password**, retype the password for the entity class.  
The password is mandatory for each entity class. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.
  - f. In **Password Validity Duration**, select the duration for which the entity class password is valid.

- g. Click **Commit** to save the changes.

System Manager displays the added entity class on the Manage Entity Classes page.

## Editing an entity class

### Procedure

1. On the System Manager web console, click **Services > Security > Certificates > Manage Entity Classes**.
2. Select an entity class, click **Edit**.
3. On the Update Entity Class page, edit the required parameters.
4. Click **Commit** to save the changes.

## Deleting an entity class

### Procedure

1. On the System Manager web console, click **Services > Security > Certificates > Manage Entity Classes**.
2. Select the entity classes, click **Delete**.  
System Manager displays the message to confirm the delete operation.
3. Click **Yes**.

System Manager deletes the selected entity class.

## Filtering entity classes

### About this task

You can apply the filter to search the values of the following columns:

- **Name**
- **Description**

### Procedure

1. On the System Manager web console, click **Services > Security > Certificates > Manage Entity Classes**.
2. Click the **Filter menu** icon, type the required value, and press **Enter**.  
The page displays the details that match the filter criteria.
3. To clear the filter values, click **Options > Clear Filter**.

System Manager clears the filter criteria.

## Manage Entity Classes field descriptions

| Name                              | Description                                                                                                                                                                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                       | The name of the entity class.                                                                                                                                                                                                                                                               |
| <b>Description</b>                | The description of the entity class.                                                                                                                                                                                                                                                        |
| <b>Password Validity Duration</b> | <p>The password validity duration of the entity class and the duration since when the password is expired.</p> <p>Following is the example, if the password:</p> <ul style="list-style-type: none"> <li>• Is still valid: 5d 6h 40m.</li> <li>• Has expired: Expired 2h 40m ago.</li> </ul> |
| <b>Whitelist Validation</b>       | <p>The white list validation status of the <b>Subject</b> field in the certificate.</p> <p>The values are:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b></li> <li>• <b>Disabled</b></li> </ul>                                                                                |

| Button                           | Description                                                     |
|----------------------------------|-----------------------------------------------------------------|
| <b>New</b>                       | Displays the Add Entity Class page to add a new entity class.   |
| <b>Edit</b>                      | Displays the Update Entity Class page to edit the entity class. |
| <b>Delete</b>                    | Deletes the selected entity class.                              |
| <b>Options &gt; Clear Filter</b> | Clears the filter criteria.                                     |
| <b>Options &gt; Columns</b>      | Customizes the display of columns.                              |
| <b>Total Records</b>             | Displays the number of available records.                       |

| Icon                                                                                                        | Description                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter menu</b> (  )  | <p>You can find the Filter menu icon next to the name of the column. You can apply the filter to search the values of the following columns:</p> <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Description</b></li> </ul>                                       |
| <b>Sorting</b> (  )      | <p>You can find this icon next to the name of the column. You can sort the values of the following columns in the alphabetical order:</p> <ul style="list-style-type: none"> <li>• <b>Name</b></li> <li>• <b>Description</b></li> <li>• <b>Password Validity Duration</b></li> </ul> |
| <b>Clear Filter</b> (  ) | Clears the filter criteria.                                                                                                                                                                                                                                                          |
|                          | Refreshes the entity classes list.                                                                                                                                                                                                                                                   |

### Related links

[manageEntityClassWhitelist command](#) on page 1204

## Add Entity Class | Update Entity Class field descriptions

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                            | <p>The name of the entity class.</p> <p>The name must be 1 to 256 characters long and can include following characters: a-z, A-Z, 0-9, -, and _. The <b>Name</b> field does not take the space.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>                     | The description of the entity class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Whitelist Validation of Subject</b> | <p>The option to enable or disable the whitelist of subject names associated with an entity class.</p> <p>You can manage the Subject Names associated with the entity class by using the <b>manageEntityClassWhitelist</b> command.</p> <p>To enable the whitelist validation, add the Subject names by using the <b>manageEntityClassWhitelist</b> command, before any enrollment.</p> <p>For information about the <b>manageEntityClassWhitelist</b> command, see “manageEntityClassWhitelist command”.</p>                                                                                                               |
| <b>Enable Password Details Update</b>  | <p>This check box is available only on the Update Entity Class page.</p> <p>In case you also want to update the password and password validity duration of the entity class, you can enable the <b>Enable Password Details Update</b> check box. When you enable the check box, System Manager displays the <b>Password Validity Duration</b> and <b>Password</b> fields.</p> <p> <b>Note:</b></p> <p>For making any changes to password details, you must update both <b>Password Validity Duration</b> and <b>Password</b> fields.</p> |
| <b>Password Validity Duration</b>      | The password validity duration of the entity class. The format of <b>Password Validity Duration</b> is Day:Hours:Minute. The maximum number of days for password validity are 28 days. This field is mandatory.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Password</b>                        | <p>The password for the entity class.</p> <p>Endpoints use this password in enrollment requests for authentication.</p> <p>You can define the password policy in the Password Policy for Programmatic Accounts section on the View and Edit Profile SMGR page.</p>                                                                                                                                                                                                                                                                                                                                                          |
| <b>Confirm Password</b>                | The password for the entity class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Button        | Description                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves any changes made in the entity class configuration.                                             |
| <b>Cancel</b> | Cancels any changes you made for add or update operation and displays the Manage Entity Classes page. |

### Related links

[View and Edit Profile SMGR field descriptions](#) on page 874

[Viewing the subject name validation status for an entity class](#) on page 1208

[Adding subject names for an entity class](#) on page 1206

[manageEntityClassWhitelist command](#) on page 1204

## manageEntityClassWhitelist command

With Release 8.1.3, you can add, list, view, and delete the subject names for the provided entity-class by using the **manageEntityClassWhitelist** command. You can add and delete the bulk entries of subject names for an entity class. Also, you can check the status of the subject name validation for the entity class.

### Syntax

```
manageEntityClassWhitelist [-h] [addAll -e <ENTITY_CLASS_NAME> -f <INPUT_FILE> -u <USERNAME> -p <PASSWORD>] [add -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -u <USERNAME> -p <PASSWORD>] [list -e <ENTITY_CLASS_NAME> -f <OUTPUT_FILE> -u <USERNAME> -p <PASSWORD> -pn <PAGENUMBER> -ps <PAGESIZE>] [view -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -f <OUTPUT_FILE> -u <USERNAME> -p <PASSWORD>] [subjectCheck -e <ENTITY_CLASS_NAME> -u <USERNAME> -p <PASSWORD>] [deleteAll -e <ENTITY_CLASS_NAME> -u <USERNAME> -p <PASSWORD>] [delete -e <ENTITY_CLASS_NAME> -s <SUBJECT_NAME> -u <USERNAME> -p <PASSWORD>]
```

**-h**

Displays help for the command and also displays the required and optional parameters.

**addAll -h -e <ENTITY\_CLASS\_NAME> -f <INPUT\_FILE> -u <USERNAME> -p <PASSWORD>**

Adds or updates the Subject Names for the provided entity class through a file for bulk operation.

**add -h -e <ENTITY\_CLASS\_NAME> -s <SUBJECT\_NAME> -u <USERNAME> -p <PASSWORD>**

Adds the Subject Names for the provided entity class.

**list -h -e <ENTITY\_CLASS\_NAME> -f <OUTPUT\_FILE> -u <USERNAME> -p <PASSWORD> -pn <PAGENUMBER> -ps <PAGESIZE>**

Lists the Subject Names for the provided entity class. You can provide a file name where System Manager can save the Subject Names.

**view -h -e <ENTITY\_CLASS\_NAME> -s <SUBJECT\_NAME> -f <OUTPUT\_FILE> -u <USERNAME> -p <PASSWORD>**

Displays the Subject Name for the provided entity class. You can provide a file name where System Manager you can save all the Subject Names.

**subjectCheck -e <ENTITY\_CLASS\_NAME> -u <USERNAME> -p <PASSWORD>**

Displays the status of the subject name validation for the entity class. The status can be enabled or disabled.

**deleteAll -h -e <ENTITY\_CLASS\_NAME> -u <USERNAME> -p <PASSWORD>**

Deletes all the Subject Names for the provided entity class.

**delete -h -e <ENTITY\_CLASS\_NAME> -s  
<SUBJECT\_NAME> -u <USERNAME> -p  
<PASSWORD>**

Deletes the specific entry of the Subject Name for the provided entity class.

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ENTITY_CLASS_NAME> | The name of the existing entity class that you create on the System Manager web console.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <SUBJECT_NAME>      | The subject name for the entity class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <INPUT_FILE>        | <p>The file name with the list of subject names and the file is available on the System Manager server. The file extension is .csv file.</p> <p>Following is an example of the format that is in the subject name file:</p> <pre>cat SubjectNameData.csv subjectName name1 name2 name3 name4 name5</pre>                                                                                                                                                                                                                                                                                                |
| <OUTPUT_FILE>       | The file name where System Manager copies and saves the details of subject names for the entity class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <USERNAMRE>         | The user name of the System Manager web console for managing the entity classes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <PASSWORD>          | <p>The password of the System Manager web console for managing the entity classes.</p> <p> <b>Note:</b></p> <p>If you do not type the <code>-u &lt;USERNAME&gt;</code> and <code>-p &lt;PASSWORD&gt;</code> parameters with the command, System Manager displays the following options after pressing Enter:</p> <pre>Enter User Name : ----- Enter Password :-----</pre> <p>When the system prompts, provide the user name and password of the System Manager web console where the entity class is configured.</p> |
| <PAGENUMBER>        | Displays the list of subject name for the provided entity class on the specific page number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <PAGESIZE>          | Displays the total number of subject names for the provided entity class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Related links

[Viewing the subject name validation status for an entity class](#) on page 1208

[Adding subject names for an entity class](#) on page 1206

## Adding subject names for an entity class

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.

2. Do one of the following:

- To add the subject name for the entity class in whitelist, type **manageEntityClassWhitelist add -e <ENTITY\_CLASS\_NAME> -s <SUBJECT\_NAME> -u <USERNAME>**, and press Enter.

Where:

- **<ENTITY\_CLASS\_NAME>**: The name of the existing entity class that you create on the System Manager web console.
- **<SUBJECT\_NAME>**: The subject name for the entity class.
- **<USERNAMRE>**: The user name of the System Manager web console for managing the entity classes.
- **<PASSWORD>**: The password of the System Manager web console for managing the entity classes.

If you do not type the **-u <USERNAME>** and **-p <PASSWORD>** parameters with the command, System Manager displays the following options after pressing Enter:

```
Enter User Name : -----
Enter Password :-----
```

When the system prompts, provide the user name and password of the System Manager web console where the entity class is configured.

For example, to add the specific entry, type the following:

```
manageEntityClassWhitelist add -e EntityClass1 -s Subject1 -u admin
```

- To add the subject name for the entity class in whitelist by using a file for bulk operation, type **manageEntityClassWhitelist addAll -e <ENTITY\_CLASS\_NAME> -f <INPUT\_FILE> -u <USERNAME>**, and press Enter.

For example, to add the entries through a file for bulk operation, type the following:

```
manageEntityClassWhitelist addAll -e EntityClass2 -f Subjectname.csv -u admin
```

3. At the **Enter Password** prompt, type the password of the System Manager web console.

System Manager adds the subject names for the entity class and displays the following message:

```
Subject name(s) added successfully
```

### Related links

[Viewing the subject name validation status for an entity class](#) on page 1208  
[manageEntityClassWhitelist command](#) on page 1204



## Displaying subject names for an entity class

### About this task

Use this procedure to list the subject names for an entity class.

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:

- To list the subject name for the entity class, type **manageEntityClassWhitelist list -e <ENTITY\_CLASS\_NAME> -u <USERNAME>**, and press Enter.

For example, to list the subject names, type the following:

```
manageEntityClassWhitelist list -e EntityClass1 -u admin
```

- To save the subject names in a file, type **manageEntityClassWhitelist list -e <ENTITY\_CLASS\_NAME> -f <output\_file> -u <USERNAME>**, and press Enter.

For example, to save the subject names in a file, type the following:

```
manageEntityClassWhitelist list -e EntityClass1 -f
SubjectNames.csv -u admin
```

3. At the **Enter Password** prompt, type the password of the System Manager web console.

System Manager displays the subject name for the entity class with the status, subjectName, and resource-uri details. It also displays the status of the subject name validation.

For example:

```
Subject name check is enabled for Entity Class : EntityClass1
Operation successful, resultSize is <2> and pageSize is <100>. Output is shown
below.
[status, subjectName, resource-uri]
[NEW, Subject1, tm-service-api/entity-classes/EntityClass1/subject-names/Subject1]
[NEW, subjectnametest, tm-service-api/entity-classes/EntityClass1/subject-names/
subjectnametest]
```

For saving the subject names in a file, System Manager displays the following message.

For example:

```
Operation successful, Output copied to <SubjectNames.csv>. ResultSize is <1> and
pageSize is <100>
```

## Viewing the subject name for an entity class

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. To view the details of the subject name for the entity class, type **manageEntityClassWhitelist view -e <ENTITY\_CLASS\_NAME> -s <SUBJECT\_NAME> -u <USERNAME>**, and press Enter.

For example, to view the specific entry detail, type the following:

```
manageEntityClassWhitelist view -e EntityClass1 -s Subject1 -u
admin
```

3. At the **Enter Password** prompt, type the password of the System Manager web console.

System Manager displays the subject name for the entity class with the status, subjectName, and resource-uri details. It also displays the status of the subject name validation.

For example:

```
Subject name check is enabled for Entity Class : EntityClass1
[status, subjectName, resource-uri]
[NEW, name1, tm-service-api/entity-classes/entity3/subject-names/name1]
```

## Viewing the subject name validation status for an entity class

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. To view the status of the subject name validation for the entity class, type **manageEntityClassWhitelist** subjectCheck -e <ENTITY\_CLASS\_NAME> -u <USERNAME> -p <PASSWORD>, and press Enter.

For example, type the following:

```
manageEntityClassWhitelist subjectCheck -e EntityClass1 -u admin
```

3. At the **Enter Password** prompt, type the password of the System Manager web console.

System Manager displays the subject name validation status. The status can be enabled or disabled.

For example:

```
Subject name check is enabled for Entity Class : EntityClass1
```

### Related links

[Adding subject names for an entity class](#) on page 1206

[manageEntityClassWhitelist command](#) on page 1204

## Deleting the subject names for an entity class

### Procedure

1. Log in to the System Manager command line interface with CLI user credentials that you create during application deployment.
2. Do one of the following:
  - To delete the specific subject name entry for the entity class, type **manageEntityClassWhitelist** delete -e <ENTITY\_CLASS\_NAME> -s <SUBJECT\_NAME> -u <USERNAME>, and press Enter.

For example, type the following:

```
manageEntityClassWhitelist delete -e EntityClass1 -s Subject1 -u
admin
```

- To delete all the subject name entries for the entity class, type **manageEntityClassWhitelist** deleteAll -e <ENTITY\_CLASS\_NAME> -u <USERNAME>, and press Enter.

For example, type the following:

```
manageEntityClassWhitelist deleteAll -e EntityClass2 -u admin
```

3. At the **Enter Password** prompt, type the password of the System Manager web console.

System Manager deletes the subject names for the entity class and displays the following message.

```
Subject name deleted successfully
```

---

## Retrieving the System Manager CA certificate

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. On the CA Functions page click **Download pem file**.
4. Click **Save** to save the certificate to a file.

---

## Certificate Authorities

### Certificate Authorities in a Geographic Redundancy setup

In System Manager configured with Geographic Redundancy, the system replicates the CA certificate from the primary System Manager server to the secondary System Manager server. By default, the primary System Manager server, the secondary System Manager server and their elements are part of the same trust domain. For the initial trust relationship, during the configuration, the secondary System Manager server uses the Certificate Enrollment password that is set on the primary server. The primary System Manager server issues a certificate to the secondary System Manager server.

When the secondary System Manager server is active, do not configure System Manager as a sub CA.

---

## Applying third-party certificates to Appliance Virtualization Platform

### About this task

Use this procedure to create, download, upload, and push third-party certificates to Appliance Virtualization Platform hosts.

### Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.
- Ensure that the certificate on the Appliance Virtualization Platform host is valid.

### \* Note:

If you are using a third-party generated CSR, add the private key for the CSR in the file `/etc/vmware/ssl/rui_csr_temp.key` before installing the certificate from Solution Deployment Manager.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

If you add the generic CSR details, the system pre-populates the values in the View/Generate CSR dialog box.

For more information about creating the generic CSR, see “Creating or editing generic CSR”.

5. To generate CSR, do the following:
  - a. Click **More Actions > AVP Cert. Management > Manage Certificate**.
  - b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
  - c. Click **View/Generate CSR**.

System Manager displays the View/Generate CSR dialog box.

- d. If the generic CSR details are not added for the Appliance Virtualization Platform host, add the details of the generic CSR.

- e. Click **Generate CSR**.

The system generates CSR for the Appliance Virtualization Platform host.

- f. In the **Current Action** column, click **Status Details** to view the status.
6. To download CSR, do the following:
  - a. Click **More Actions > AVP Cert. Management > Manage Certificate**.
  - b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
  - c. Click **Download CSR**.
 

In case of Firefox browser, the system prompts you to save the `CSR.zip` file.
  - d. In the **Current Action** column, click **Status Details** to view the status.
 

In the Download CSR Status dialog box, the system displays the path of the downloaded `CSR.zip` file.
7. Extract the downloaded certificates, and ensure that the third-party signs them.
8. To upload and push the signed certificate from a third-party CA, do the following:
  - a. Click **More Actions > AVP Cert. Management > Manage Certificate**.
  - b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
  - c. Click **Browse** and select the required certificates from the local computer.
  - d. Click **I Agree to accept to add the same certificate in SDM**.
  - e. Click **Push Certificate**.
  - f. In the **Current Action** column, click **Status Details** to view the status.

---

## Creating or editing generic CSR

### About this task

Use this procedure to create or edit a generic CSR for third-party Appliance Virtualization Platform certificates. With a generic CSR, you can apply the same set of data for more than one Appliance Virtualization Platform host.

### Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click **More Actions > AVP Cert. Management > Generic CSR**.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click **Create/Edit CSR** and then click **OK**.

## Next steps

Complete the CSR generation, download, third-party signing and push the certificates to the Appliance Virtualization Platform hosts.

---

# Generating certificates from System Manager

## Certificate generation

Generation of certificates from the System Manager web console includes the following tasks:

- (Optional) Creating a certificate signing request (CSR).
- Creating an end entity.
- Generating the certificate keystore.
- Creating the certificate using CSR.
- Viewing contents of the certificate.

## Creating a certificate signing request

### Before you begin

Install the OpenSSL command line tool.

### About this task

Perform this procedure if you want to generate the certificate with the key that you generate and get System Manager to sign your keys.

Do not perform the procedure if you want System Manager to generate the public and private keys for the certificate.

### Procedure

1. Start an SSH session on System Manager.
2. To generate the keys and a corresponding certificate signing request (CSR), type the following command:

```
openssl req -out <CSR name> -new -newkey rsa:2048 -nodes -keyout <PvtKey_Filename>
```

Where:

- CSR name is the name of the output CSR file. For example, `mycsr.csr`.
- `rsa:2048` instructs the system to create a 2048-bit RSA key.
- `PvtKey_Filename` is the filename where the system stores the private key. For example, `privateKey.key`.

## Creating an end entity

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **RA Functions > Add End Entity**.
4. On the Add End Entity page, in **End Entity Profile**, select **INBOUND\_OUTBOUND\_TLS**.
5. Type the username and password.

The password is mandatory for each end entity. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.

6. Enter the relevant information in the fields.

The system automatically selects the following:

- **ID\_CLIENT\_SERVER** in **Certificate Profile**
- **tmdefaultca** in **CA**
- **User Generated** in **Token**

With **User Generated**, the system generates the certificate by using CSR. You can also select **P 12 file**.

7. Click **Add**.

The system displays the message `End Entity <username> added successfully`.

## Generating the certificate keystore

### Before you begin

Create an end entity.

For more information, see [Creating an end entity](#).

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. In the navigation pane, click **Public Web**.
4. On the public EJBCA page, do one of the following:
  - If you are generating the certificate by using certificate signing request (CSR), click **Enroll > Create Certificate from CSR** and continue with the steps in [Creating the certificate by using certificate signing request](#).
  - Do the following:
    - Click **Enroll > Create Keystore**.

- On the Keystore Enrollment page, type the username and password.

**\* Note:**

Provide the same username and password that you entered while creating the end entity on the Add End Entity page.

- Click **OK**.
- On the next page, retain the values in the **Key length** field, and click **OK**.

The system generates a PKCS12 format keystore with the identity certificate that contains values provided in the end entity.

## Related links

[Creating an end entity](#) on page 1213

## Creating the certificate using a CSR

### Before you begin

Create an end entity as described in [Creating an end entity](#) on page 1213.

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. In the navigation pane, click **Public Web**.



4. On the public EJBCA page, click **Enroll > Create Certificate from CSR**.
5. To get your certificate, on the Certificate Enrollment from a CSR page, do the following:
  - a. Enter the same username and the password that you provided while creating the end entity.
  - b. In the text box, paste the PEM-formatted PKCS10 certification request.
  - c. Click **OK**.

A certificate in PEM format is generated. The certificate contains the values provided in the end entity.

#### Related links

[Creating an end entity](#) on page 1213

## Viewing contents of the certificate

### Before you begin

Install the tool that you want to use to view the keystore.

### About this task

You can view the contents of the certificate in a keystore by using any common tool, such as keytool.

### Procedure

1. Start an SSH session.
2. To view the contents of the certificate in a keystore, type the following command:

```
keytool -list -keystore <keystore> -storepass <keystorepassword> -storetype PKCS12 -v
```

Where:

- keystore is the path to the keystore.
- keystorepassword is the password of the keystore
- PKCS12 is the format of the keystore. Use JKS for the JKS format keystores.

3. To view the contents of a PEM certificate, type the following command:

```
openssl x509 -in <certificate> -text noout
```

Where: certificate is the path to the PEM certificate.

## Overview of System Manager root certificate authority created using SHA256withRSA signing algorithm and 2048 key size

System Manager that is upgraded from releases earlier than Release 7.0, contains root Certificate Authority (CA) that has a key size of 1024 bits and uses the SHA1withRSA algorithm for signing own certificates.

You can use the createCA utility to improve the level of security of the System Manager CA by updating the key size to 2048 bits and the algorithm to SHA256withRSA.

Before running the utility, note the following:

- You must not use the createCA utility of one release on another release.
- If you upgrade System Manager after running the createCA utility, you do not need to run this utility again on the upgraded System Manager as the CA is carry forwarded as part of the upgrade process.
- You can use the utility in the following conditions:
  - When the System Manager root CA has been compromised.
  - Or, when you want to upgrade the signing algorithm and key size of the System Manager root CA.

**+ Tip:**

When you run the utility, the system displays a message along with the signing algorithm information that is used to create the existing root CA. If the signing algorithm is SHA256withRSA, then you do not need to run this utility.

- Starting from System Manager Release 7.0, the createCA utility can be run in a phased manner with the help of different options provided with the utility. The utility has the following options:
  - Option 1: Allows you to create a new root CA using SHA256withRSA signing algorithm and 2048 key size.
  - Option 2: Allows you to make the new root CA the default CA of System Manager.
  - Option 3: Allows you to run a single step process where the system creates a new root CA using SHA256withRSA signing algorithm and 2048 key size and makes that CA the default System Manager CA.

**\* Note:**

- You should select option 3 in the createCA utility for smaller deployments which have limited number of elements configured with the System Manager.
  - You should not select option 3 to create a new root CA in case you have run the utility by selecting option 1, and option 2.
- Option 4: Allows you to exit the utility.
- Running the utility in a phased manner allows you to obtain the new root CA certificate after the first phase (option 1), and distribute the certificate to all the TLS connected elements before selecting option 2.
- To minimize service interruptions on a production network, it is recommended to run the utility by using option 1, distribute the certificate to all TLS connected elements, and then run the utility by using option 2.

## Creating a new Certificate Authority by using SHA256withRSA signing algorithm and 2048 key size

### Before you begin

Ensure that:

- You have read this section properly and have understood the implications of creating a new root Certificate Authority to issue certificates.

For more information, see [Overview of System Manager root certificate authority created using SHA256withRSA signing algorithm and 2048 key size](#) on page 1215.

- System Manager Release 7.0 or later is installed.

**\* Note:**

- The createCA utility is available in System Manager starting from Release 6.3.8.
- If you are on a release earlier than Release 7.0, you must upgrade the System Manager to the latest release before running the utility. The utility is not available for System Manager releases earlier than 6.3.8. For details about running the utility in System Manager versions earlier than 7.0, refer the corresponding *Administering Avaya Aura® System Manager* document.
- You have taken backup of the System Manager virtual machine before running the utility. If you are on Release 6.3.x of System Manager running on System Platform, ensure to take a backup from the System Manager UI and System Platform UI before running the utility.
- You have disabled the Geographic Redundancy replication for System Manager. You should re-configure Geographic Redundancy after executing option 1 followed by option 2 in the phased manner or after executing option 3 in the single step approach.

For more information, see “Geographic Redundancy”.

## Procedure

1. On the System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. If the system prompts you to run the utility, type `y`.
4. Based on your requirement, type the appropriate option:
  - 1 to create a new root CA.
  - 2 to make the new root CA the default System Manager CA.
  - 3 to create a new root CA and then, make that new root CA the default System Manager CA in a single step.
  - 4 to exit from this utility.

## Related links

[Creating a new CA using option 1 of the createCA utility](#) on page 1217

[Making the new CA as default System Manager CA using option 2 of the createCA utility](#) on page 1220

[Creating a new CA using option 3 of the createCA utility](#) on page 1221

## Creating a new CA using option 1 of the createCA utility

### About this task

Use this procedure to create a new CA with SHA256withRSA signing algorithm and keysize of 2048 bits.

## Procedure

1. On the System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. When the system prompts, type `y`.
4. Type `1` to create a new root CA.
5. When the system prompts, type `y`.
6. Type the Common Name (CN) of the new CA.

 **Note:**

The default CN of the new CA is `SystemManager CA`.

7. Type `y` to confirm the provided Common Name.

The system creates a new CA with the name `CreateCA`.

## Next steps

Access the new CA by logging in to the System Manager web console.

For more information, see [Downloading the new root CA](#) on page 1218.

### ***Downloading the new root CA***

#### Procedure

1. Log in to the System Manager web console with the customer login credential which have administrative privileges.
2. Click **Services > Security > Certificates > Authority > CA Structure & CRLS**.
3. Click **Download PEM file** to download the root CA to your desired location.

## Next steps

Ensure that you place the new CA in the trusted stores of following elements, which:

- Communicate with System Manager using TLS.
- Get identity certificate issued by the System Manager CA.

 **Note:**

For details about placing the CA in trusted stores of elements, see [Prerequisites before making the new root CA as the default CA of System Manager](#) on page 1218.

### ***Prerequisites before making the new root CA as the default CA of System Manager***

1. Place the new root CA in the trusted stores of elements which communicate with System Manager using TLS, and which get identity certificate issued by the System Manager CA.  
Elements, such as SIP endpoints, Communication Manager communicate with System Manager using TLS.

Elements, such as, Session Manager, Session Border Controller get identity certificate issued by the System Manager CA.

To add the new System Manager root CA certificate to Communication Manager trust store, see [Distributing the new root CA with Communication Manager](#) on page 1219.

To add the new System Manager root CA certificate to the trust store of 96x1 series phones, see [Distributing the new root CA with 96x1 series phones](#) on page 1219.

 **Note:**

Ensure that all other devices that connect using TLS to System Manager or any other server using the System Manager CA issued certificate also trust the new root CA. For detailed description on how to add a trusted certificate to those devices, refer the corresponding product documentation.

2. Disable the Geographic Redundancy replication for System Manager and convert the primary System Manager server to a standalone server.

For more information, see [Disabling the Geographic Redundancy replication for System Manager and converting the primary server to a standalone server](#) on page 1220.

## Distributing the new root CA with Communication Manager

### About this task

Use this procedure to add the new System Manager root CA certificate to the trust store of Communication Manager.

### Procedure

1. Log in to the Communication Manager SMI with administrative credentials.
2. Click **Miscellaneous > Download Files**.
3. Select the \*.pem file, and click **Download**.
4. On the SMI, click **Security > Trusted Certificates**.
5. Click **Add**.
6. Type the file name that you uploaded and click **Open**.
7. On the next screen, type a file name with \*.crt extension and select the Communication Manager repository check box.
8. Click **Add**.
9. Restart the Communication Manager system.

## Distributing the new root CA with 96x1 series phones

### About this task

Use this procedure to add the new System Manager root CA certificate to the trust store of 96x1 series phones.

## Procedure

1. Search for the IP address or Fully Qualified Domain Name (FQDN) of the HTTP server from where the 96x1 series phones download the `settings` file.
2. Upload the new System Manager root CA certificate on the server.
3. Open the `settings` file on a text editor (for example, Notepad), and type the new root CA file name next to the SET TRUSTCERTS parameter.

 **Note:**

Ensure that the name of the older root CA is also present next to the SET TRUSTCERTS parameter.

4. Save and close the `settings` file.
5. Restart the phones.

Disabling the Geographic Redundancy replication for System Manager and converting the primary server to a standalone server

## Procedure

1. Disable the Geographic Redundancy replication for System Manager.  
For more information, see “Disabling the Geographic Redundancy replication”.
2. Convert the primary System Manager server to a standalone server.  
For more information, see “Converting the primary System Manager server to the standalone server”.

### ***Making the new CA as default System Manager CA using option 2 of the createCA utility***

#### About this task

Use this procedure to make the new CA as the default System Manager CA and issue new certificates for System Manager services by using the new CA.

 **Note:**

After performing this task, the System Manager web console will be unavailable for approximately 15 minutes.

## Procedure

1. On System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. When the system prompts, type `y`.
4. Type `2` to make the new CA the default System Manager CA.
5. When the system prompts, type `y`.

The CA that was created after typing option 1 is renamed as `tmdefaultca` and this CA becomes the default CA of System Manager.

6. **(Optional)** To download the CA, log in to the System Manager web console, and click **Services > Security > Certificates > Authority > CA Structure & CRLS > tmdefaultca**.

### Next steps

Manage all the tasks that must be performed after selecting options 1 and 2 in the createCA utility. For more details, see [Managing tasks after running the createCA utility](#) on page 1222.

### Creating a new CA using option 3 of the createCA utility

#### About this task

This task sequentially performs all the actions that can be achieved by selecting options 1 and 2 in the createCA utility.

#### \* Note:

- You should select option 3 in the createCA utility for smaller deployments which have limited number of elements configured with the System Manager.
- You should not select option 3 to create a new root CA in case you have run the utility by selecting option 1, and option 2.

#### Procedure

1. On the System Manager CLI, start an SSH session by logging in with customer login credentials.
2. Type `createCA`.
3. When the system prompts, type `y`.
4. Type `3` to create a new root CA and make that CA as the default System Manager CA.
5. When the system prompts, type `y`.

The new root CA that is created is renamed as `tmdefaultca` and this CA becomes the default CA of System Manager.

6. To download the CA, log in to the System Manager web console and click **Services > Security > Certificates > Authority > CA Structure & CRLS > tmdefaultca**
7. Distribute the new root CA with other elements, for example, Communication Manager, 96x1 series phones, Session Manager, Session Border Controller and so on.
8. Disable the Geographic Redundancy replication for System Manager and convert the primary System Manager server to a standalone server.
9. Manage the tasks that must be performed after running the createCA utility.

#### Related links

[Distributing the new root CA with Communication Manager](#) on page 1219

[Distributing the new root CA with 96x1 series phones](#) on page 1219

[Disabling the Geographic Redundancy replication for System Manager and converting the primary server to a standalone server](#) on page 1220

[Managing tasks after running the createCA utility](#) on page 1222

## Managing tasks after running the createCA utility

### Before you begin

Ensure that you have run the createCA utility using one of the following procedures:

- Using option 1 followed by using option 2 in the phased approach.
- Using option 3 in the single step approach.

### Procedure

1. Set the enrolment password which is reset after running the createCA utility.

 **Note:**

For more information, see “Setting the enrollment password”.

2. To configure the System Manager Geographic Redundancy, perform the following:
  - a. Convert the primary System Manager server to a standalone server.
  - b. Reinstall the secondary System Manager.
  - c. Re-configure Geographic Redundancy by logging in to the web console of the secondary System Manager.

 **Note:**

For more information, see “Geographic Redundancy”.

3. Regenerate new certificates for elements that use System Manager issued certificates. For example, if your network consists of two core Session Manager systems, then perform the following steps:
  - a. Log in to the System Manager web console.
  - b. Change the service state for the primary Session Manager to **Deny New Service**. For more details, refer *Administering Avaya Aura® Session Manager*
  - c. Log in to the primary Session Manager CLI and System Manager CLI.
  - d. Type `initTM -f`.
  - e. On the System Manager CLI, type `service jboss restart` to restart the System Manager JBOSS server.

After you run the above command, the System Manager web console will be inaccessible for approximately 15 minutes.

- f. For SIP Endpoints, regenerate the SIP and HTTP certificates using the "enhanced validation" certificates on Session Manager.

For more information, see the “Installing Enhanced Validation Certificates for Session Manager” section in the *Administering Avaya Aura® Session Manager* document.

- g. Change the service state for the primary Session Manager to **Accept New Service**.

For more information, see *Administering Avaya Aura® Session Manager*



- h. Repeat above steps for the secondary Session Manager.
- 4. To delete the old System Manager CA, perform the following:
  - a. Log in to the System Manager web console with customer login credentials which have administrative privileges.
  - b. Click **Services > Security > Certificates > Authority > Certification Authorities**.
  - c. Select the older CA.
 

The older CA may appear as `olddefaultcaXXX` after the new root CA is set as the default System Manager CA.
  - d. Click **Delete CA**.

**Warning:**

It is an irreversible step. Ensure that you have placed the latest root CA on the trusted stores of all the elements before deleting the older CA.

- 5. To regenerate new certificates for Presence Services servers starting from Release 6.2.x, perform the following:
  - a. Log in to the CLI of the Presence Services server.
  - b. Type `prescert reconfigureAll scep pw <smgr_enrollment_passwd>`.
  - c. Type `stop.sh`.
  - d. Type `start.sh`.
- 6. Generate a new identity certificate for any other server, for example, Session Border Controller that are configured in the network and that use System Manager issued certificates.
 

For more information, refer to the corresponding product documentation.
- 7. Delete the old CA certificate from System Manager trust stores.
 

For more information, refer “Removing trusted certificates”.
- 8. Delete the old CA certificate from the trust store of endpoints, Communication Manager and any other element that trusted it.

---

## External SSL configurations in System Manager

### Using a third-party identity certificate for System Manager

From the System Manager web interface, you can install an identity certificate for System Manager issued by a certificate authority (CA). After the certificate installation, during SSL communications, System Manager presents the identity that is issued by the third-party identity certificate.

Installing and using the third-party identity certificate for the System Manager web interface includes the following key tasks:

1. Replacing the System Manager web server certificate with a third-party certificate.
2. Updating the truststores for internal services, clients, or managed elements with third-party root and subordinate CA certificate.

For more information about installing the third-party identity certificate, see *Avaya Aura® System Manager Certificate Management* on the Avaya Support site at <http://support.avaya.com>.

---

## Set the System Manager CA as the subordinate CA

### **Note:**

Before you begin, ensure you take a snapshot of the System Manager application. Once the subordinate CA (SubCA) has been successfully set up and you have verified all the functionalities, ensure you remove the snapshot of the System Manager application.

You can change the default Certificate Authority (CA) that the system generates during the System Manager installation to an externally signed SubCA. Using this capability, you can add System Manager CA to an existing CA hierarchy in the customer environment.

In a Geographic Redundancy enabled system, EJBCA configured as SubCA on the primary System Manager server is also provisioned on the secondary System Manager server.

### **Note:**

System Manager as a certificate authority does not support Delta CRLs and the Avaya Aura® elements also do not validate Delta CRL. Therefore, do not create Delta CRL from System Manager.

The **Extended Key Usage** field should not be set in the SubCA certificate.

### Related links

[Generating the certificate signing request](#) on page 1224

[Guidelines for signing the certificate signing request](#) on page 1225

## Generating the certificate signing request

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > Certification Authorities**.
4. On the Manage Certification Authorities page, in **Add CA**, type the name `ExternalSubCA`, and click **Create**.
5. On the Create CA page, do the following:
  - a. In **Type of CA**, select **X509**.

- b. In **Signing Algorithm**, select **SHA256WithRSA**

 **Note:**

Do not use anything else.

- c. In **Crypto Token**, retain the default value.
- d. In **Description**, provide a description.
- e. In **Enforce unique DN**, clear the check box.
- f. In **Subject DN**, type a DN for your SubCA.

For example, CN=ExternalSubCA,O=AVAYA,C=US.

 **Important:**

Entering incorrect values in **Subject DN** can lead to failures.

- g. In **Signed By**, click **External CA**.

6. In the **Externally signed CA creation/renewal** section, click **Browse**, and open the CA certificate file that is on your computer.

 **Note:**

You must have the CA certificate that is used to sign the CA. If the external signing CA is a SubCA, then you need to ensure that you use the full chain in its certificate hierarchy, all the way to the root CA. The certificate chain must be in the PEM format and available on the same computer on which you run the browser.

7. Click **Make Certificate Request**.

You receive a request for a PEM-formatted certificate.

8. Click **Download PEM file**.

9. Click **Save File**, and save the file on your computer.

## Guidelines for signing the certificate signing request

Following are the guidelines for the certificate signing request:

- Use the -preserveDN flag while executing the `openssl ca` command to sign the request.

 **Note:**

By default, Openssl reorders DN to whatever the Openssl policy file is set up to do. Use the -preserveDN flag while you sign the request by running the `openssl ca` command. If you do not use the -preserveDN flag, EJBCA does not recognize the CA and the certificate request fails.

- You must set `basicConstraints=CA:TRUE` for the signed certificate while signing the request.
- You must get the certificate request signed by using the SHA256WithRSA Signing Algorithm
- You must ensure the CA-signed certificate contains proper revocation related information in it. Ensure that the revocation checking URLs are correct and reachable from the elements interacting with System Manager CA.

## Receiving certificate response

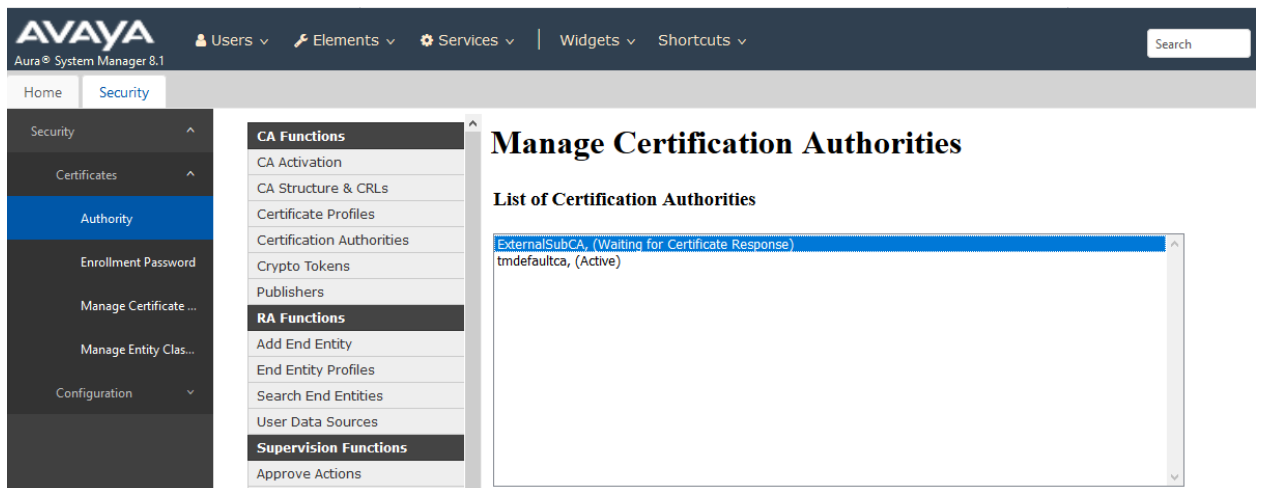
### Before you begin

Ensure that the received SubCA certificate is properly signed by the authorised CA. To check, use the openssl command.

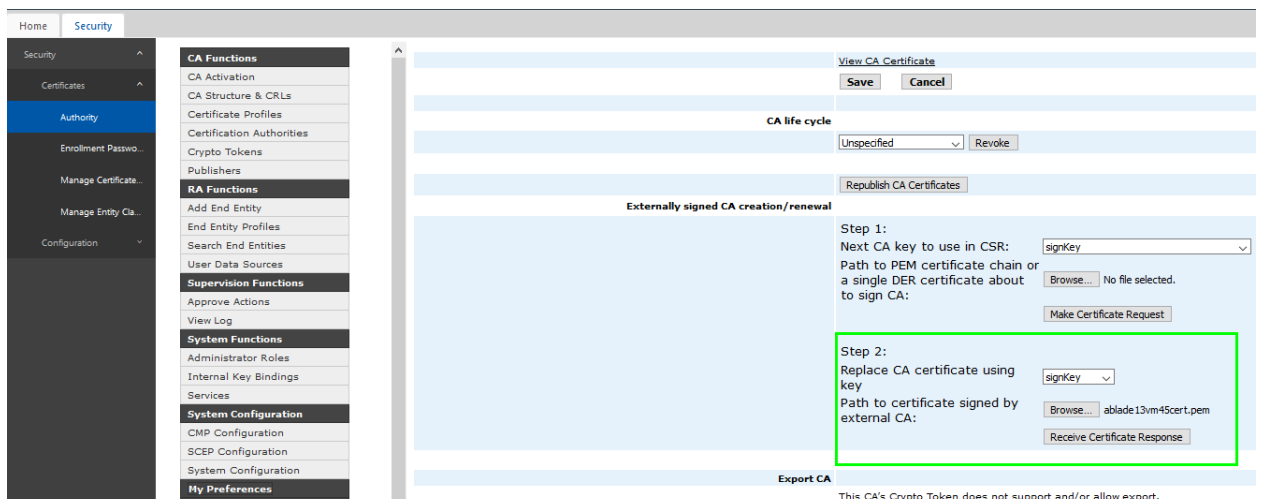
```
openssl verify -CAfile ca-cert.pem subca-cert.pem
```

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > Certification Authorities**.
4. Select **ExternalSubCA** that you created earlier with the “Waiting for Certificate Response” status, and click **Edit CA**.

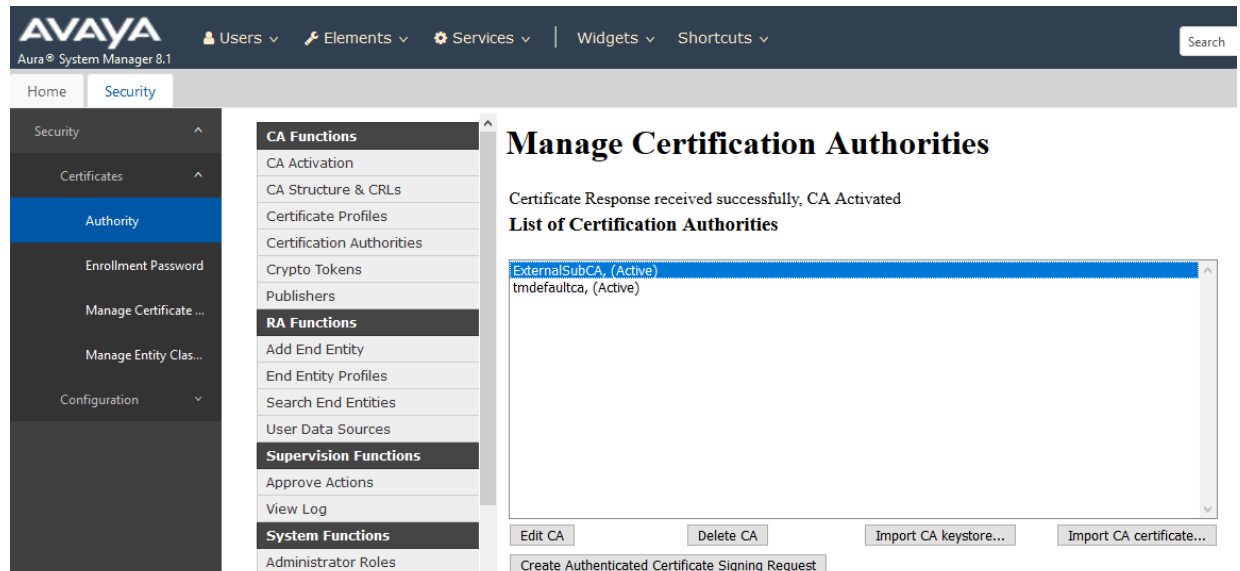


5. In the Externally signed CA creation/renewal section, in **Path to certificate signed by external CA**, click **Choose File**, and browse to the signed certificate.



## 6. Click **Receive Certificate Response**.

The system displays a message that the certificate response is received successfully and that the CA is activated. If you do not see this message, double-check the contents of the certificate file.



## Configuring revocation information in the subordinate CA

### About this task

It is not mandatory but Avaya recommends configuring revocation information in the SubCA.

### Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the navigation pane, click **Certificates** > **Authority**.
3. Click **CA Functions** > **Certification Authorities**.
4. Select ExternalSubCA that you created earlier, and click **Edit CA**.
5. On the Edit CA page, fill values only in these two fields, **Default OCSP Service Locator** and **Default CRL Dist. Point**.
6. In **Default OCSP Service Locator**, add the following value:

`http://<SMGR_VFQDN>/ejbca/publicweb/status/ocsp`

### \* **Note:**

Replace SMGR\_VFQDN with the appropriate System Manager VFQDN.

Delta CRL Period (\*y \*mo \*d \*h \*m) [?] 0m y=365 days, mo=30 days  
(0m, if no delta CRLs are issued)

CA issuer URI [?]

Publishers

Services

Default OSCP Service Locator [?] <http://grsmgr.dsmgrsv.com/ejbca/publicweb/status/ocsp>  
(used as default value in certificate profiles using this CA)

CMS Service ☐ Activate

Other data

Approval Settings

Add/Edit End Entity  
Key Recovery  
Revocation  
CA Service Activation

7. To find the System Manager VFQDN, access the URL `https://{system-manager-fqdn}/ws/grservice/getgrstate/test` on the browser.

It returns a value like the following:

STANDALONE 172.19.17.1 ablade13vm1.dsmgrsv.com STANDALONE 127.0.0.1  
grsmgr.dsmgrsv.com 8.1.7.813011765 2020-09-23T13:57:33.445Z

Here *grsmgr.dsmgrsv.com* is the VFQDN, the value before the release number text.

8. Add a value in the **Default CRL Dist. Point**. For deriving the value, replace the last part of the text, `http://<SMGR_VFQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=url-encoded-issuerD`, do as follows:

### CA Structure & CRLs

Basic Functions for CA : ExternalSubCA [View Certificate](#) [View Information](#)

Root CA : CN=nageshsmgrsvopenspca,OU=Telecom,O=Avaya,L=Pune,ST=MH,C=IN  
[Download binary/to IE](#) [Download to Firefox](#) [Download PEM file](#)

Subordinate CA, level 1 : CN=ExternalSubCA,O=AVAYA,C=US  
[Download binary/to IE](#) [Download to Firefox](#) [Download PEM file](#)

Latest CRL: Created 2020-09-23 19:22:41+05:30, Expires 2020-09-24 19:22:41+05:30, number 1 [Get CRL](#)  
Delta CRLs are not enabled.

Create a new updated CRL :

Open Link in New Tab  
Open Link in New Window  
Open Link in New Private Window  
Bookmark This Link  
Save Link As...  
Save Link to Pocket  
Copy Link Location  
Search Google for "Get CRL"  
Send Link to Device  
This Frame  
Inspect Accessibility Properties  
Inspect Element (Q)

- On CA Functions page, click **CA Structure & CRLs**.
- In the **ExternalSubCA** that you created earlier. On **Get CRL**, right-click and select **Copy link address**.

- c. Paste the contents in a Notepad, [https://<SMGR\\_IPAddress>/ejbca/adminweb/ca/getcrl/getcrl?cmd=crl&issuer=CN%3DExternalSubCA%2CO%3DAVAYA%2CC%3DUS](https://<SMGR_IPAddress>/ejbca/adminweb/ca/getcrl/getcrl?cmd=crl&issuer=CN%3DExternalSubCA%2CO%3DAVAYA%2CC%3DUS)
9. Copy everything after issuer= and paste it after issuer= in the earlier URL.

**\* Note:**

<http://<grsmgr.dsmgrsv.com>/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN%3DExternalSubCA%2CO%3DAVAYA%2CC%3DUS>

Place this URL in the box **Default CRL Dist. Point**.

The screenshot shows the 'CA Functions' menu on the left, with 'Certification Authorities' selected. The main area displays the configuration for a CA. The 'Default CRL Dist. Point' field is highlighted with a green box and contains the URL: <http://grsmgr.dsmgrsv.com/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN%3DExternalSubCA%2CO%3DAVAYA%2CC%3DUS>. Below this field, it says '(used as default value in certificate profiles using this CA)'. Other fields like 'Name Constraints, Excluded' and 'Default CRL Issuer' are also visible.

10. Click **Save**.

## Setting the new CA as the default CA

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > Certification Authorities**.
4. Select the new Sub CA, ExternalSubCA, and ensure that the status is **Active**.
5. On the Manage Certification Authorities page, to rename the existing CA, tmdefaultca, do the following:
  - a. From the list, highlight tmdefaultca.
  - b. In the text box at the bottom of the page, type in a new name. For example, oldtmdefaultca.
  - c. Click **Rename**.

 **Important:**

The CRD files refer to tmdefaultca. Therefore, rename the CA that you want to make as default to tmdefaultca.

6. To rename ExternalSubCA to tmdefaultca, do the following:
  - a. From the list, highlight ExternalSubCA.
  - b. In the text box at the bottom of the page, type `tmdefaultca`.
  - c. Click **Rename**.

The system sets your new ExternalSubCA as the default CA.

### Next steps

Create a backup. For more information, see "[Creating a data backup](#) on page 842".

## Modifying the default end entities to use the new CA

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > Certificate Profiles**.
4. For **ID\_CLIENT**, click **Edit**.
5. On the Edit page, in **Available CAs**, highlight tmdefaultca.
6. Click **Save**.
7. On the Manage Certificate Profiles page, repeat Step 4 through Step 6 for **ID\_CLIENT\_SERVER** and **ID\_SERVER**.
8. Click **RA Functions > Edit Entity Profiles**.
9. Select **INBOUND\_OUTBOUND\_TLS** and click **Edit End Entity Profile**.
10. On the Edit End Entity Profile page, in **Default CA**, select tmdefaultca.
11. In **Available CAs**, highlight tmdefaultca.
12. Click **Save**.
13. Repeat Step 9 through Step 12 for **INBOUND\_TLS**, **OUTBOUND\_TLS**, and **EXTERNAL\_CSR\_PROFILE**.
14. Click **RA Functions > Search End Entities**.
15. On the Search End Entities page, in **Search end entities with status**, click **All**.
16. Click **Search**.
17. Ensure that the list contains the end entities: **INBOUND\_OUTBOUND\_TLS**, **INBOUND\_TLS**, **OUTBOUND\_TLS**, and **EXTERNAL\_CSR\_PROFILE**.



If the required end entity is unavailable:

- Geographic Redundancy configuration might fail.
- The system displays the message: The secondary System Manager server is unable to POST a CSR for signing.
- The primary System Manager server error log displays the message: Unable to sign csr for user `EXTERNAL_CSR_PROFILE, 1, ...`

18. On the Search End Entities page, for each end entity listed in the earlier step, do the following:

- a. Click **Edit End Entity**.
- b. On the Edit End Entity Profile page, in the **CA** field, ensure that the value is set to `tmdefaultca`.
- c. Click **Save**.

19. Click **Close**.

20. On the Search End Entities page, click **Reload**.

The system displays the new value in the **CA** column for all the four entities.

## Adding root CA and subordinate CAs to the trusted stores

### About this task

After the new subordinate CA is created, add the root and all intermediate CA certificates in its chain to 'All' the trusted stores of System Manager.

#### **Note:**

Add the root and all intermediate CA certificates to all elements in the network that interact with System Manager CA-issued certificates.

### Procedure

1. Log in to the System Manager web console with administrator privilege credentials.
2. Click **Services > Security > Certificates > Authority**.
3. Click **CA Structure & CRLs** link.
4. For the CA = "tmdefaultca", download the PEM file for the root CA and all subordinate CA(s) by clicking on **Download PEM file** link associated with each CA.

Refer to the document for the respective products on how to add the certificates to the store.

For adding certificates into 'All' truststores of System Manager, see [Adding trusted certificates](#) on page 1184

## Generating new identity certificates for System Manager

### About this task

After CA is set up to issue certificates by using the new Subordinate CA, update the identity certificates that are created for System Manager during the initialization of System Manager. These certificates are signed by tmdefaultca, and not by the new CA. Also, the new CA must be added to the System Manager truststores.

### Procedure

1. Replace all the Service Names listed under **Manage identity certificates** with new CA-signed certificates.

See "Replacing an identity certificate". Verify the certificates as you replace them. Do not check the **Common Name(CN)** and **Subject Alternative Name(SAN)** check boxes, if they are proper.

 **Note:**

While replacing Identity certificates, select the **Replace this Certificate with Internal CA Signed Certificate** option, select **Common Name(CN)**, and **Subject Alternative Name(SAN)** fields with default values. Select **Key Algorithm** as RSA and **Key Size** as 2048.

 **Note:**

Replace the container\_tls service certificate at the end. After replacing this certificate, you need to restart the JBoss service immediately.

2. Restart JBoss service on the System Manager server.

## Confirming identity certificate updates on System Manager

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. On the Manage Elements page, select a System Manager instance, and click **More Actions > Manage Identity Certificates**.
3. On the Identity Certificates page, select any of the certificates, and verify that the **Issuer Name** in the window below is the DN of your new CA.
4. On the Manage Elements page, select a System Manager instance, and click **More Actions > Manage Trusted Certificates**.

On the Trusted Certificates page, the system must display one certificate with DN of your new CA certificate in each of the StoreTypes. The system must display three instances on this page.

Restart all System Manager applications JBoss and systemMonitor so that the new certificates are read. Alternatively, you can reboot the System Manager server.

5. To restart System Manager applications, reboot the System Manager server.

The System Manager CA changes from the internally generated CA to an externally signed SubCA.

6. **(Optional)** In a Geographic Redundancy setup, reconfigure the System Manager secondary server.

---

## Configuring DTLS for CS 1000

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select the CS 1000 element.
4. Click **More Actions > Manage Identity Certificates**.
5. Select the Dtls and click **Replace**.
6. Select **Replace this Certificate with Internal CA Signed Certificate** and provide the common name, keysize, and the algorithm.
7. Click **Commit**.

---

## Configuring SIP TLS for CS 1000

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select the CS 1000 element.
4. Click **More Actions > Manage Identity Certificates**.
5. Select SipTls and click **Replace**.
6. Select **Replace this Certificate with Internal CA Signed Certificate** and provide the common name, keysize, and the algorithm.
7. Click **Commit**.

---

## Managing certificate revocation list

### Creating a new CRL

#### About this task

You can create a new updated Certificate Revocation List (CRL) to immediately revoke or unvoke a certificate issued by System Manager as a certificate authority.

 **Note:**

System Manager as a certificate authority does not support Delta CRLs and the Avaya Aura® elements also do not validate Delta CRL. Therefore, do not create Delta CRL from System Manager.

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > CA Structure & CRLs**.
4. Click **Create CRL**.

The system creates an updated CRL and displays the time stamp of the updated CRL.

5. Click **Get CRL**.

The **Certificate Revocation List** dialog box displays the serial numbers of revoked certificates.

## Configuring CRL download

### About this task

You can schedule a download job to periodically download the updated CRL to check for revoked or unrevoked certificates.

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Configuration > CRL Download**.
3. On the CRL Download Configuration page, click **Add**.

The system displays the Schedule CRL Download page.

4. In **Job Name**, type the job name.
5. In **Job Frequency**, set the frequency, and recurrence.

For more information, see Schedule CRL Download field descriptions.

6. In **Configure CRL Distribution Point**, type the CRL distribution point URL, and click **Add**.
7. Click **Commit**.

### Related links

[Schedule CRL Download field descriptions](#) on page 1234

### Schedule CRL Download field descriptions

| Name               | Description                                           |
|--------------------|-------------------------------------------------------|
| <b>Job Details</b> | Expands and collapses the <b>Job Details</b> section. |

*Table continues...*

| Name                                    | Description                                                                |
|-----------------------------------------|----------------------------------------------------------------------------|
| <b>Job Frequency</b>                    | Expands and collapses the <b>Job Frequency</b> section.                    |
| <b>Configure CRL Distribution Point</b> | Expands and collapses the <b>Configure CRL Distribution Point</b> section. |
| <b>Expand All</b>                       | If collapsed, expands all the sections.                                    |
| <b>Collapse All</b>                     | If expanded, collapses all the sections.                                   |

## Job Details

| Name            | Description                   |
|-----------------|-------------------------------|
| <b>Job Name</b> | The name of the download job. |

## Job Frequency

| Name              | Description                                                    |
|-------------------|----------------------------------------------------------------|
| <b>Task Time</b>  | Options to select the date, time, and time zone.               |
| <b>Recurrence</b> | Options to set the recurrence of the download job.             |
| <b>Range</b>      | Options to set the date range for the end of the download job. |

## Configure CRL Distribution Point

| Name                          | Description                                                       |
|-------------------------------|-------------------------------------------------------------------|
| <b>CRL Distribution Point</b> | The option to enter a single or multiple CRL distribution points. |

| Icon                                                                                | Description                                                            |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------|
|  | Refreshes the information of the CRL distribution points in the table. |

| Button          | Description                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------|
| <b>Add</b>      | Validates and adds the entered CRL distribution point.                                                   |
| <b>Show</b>     | Shows the selected number of CRL distribution points.                                                    |
| <b>Previous</b> | Displays the CRL distribution points on the previous page. This button is unavailable on the first page. |
| <b>Next</b>     | Displays the CRL distribution points on the next page. This button is unavailable on the last page.      |
| <b>Commit</b>   | Creates the CRL download job and displays the CRL Download Configuration page.                           |
| <b>Cancel</b>   | Displays the CRL Download Configuration page with all the details of the download job.                   |

## Related links

[Configuring CRL download](#) on page 1234

## Deleting a CRL download job

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Configuration > CRL Download**.  
The system displays the CRL Download Configuration page.
3. In **CRL Download Jobs**, select a job and click **Delete**.
4. In the Confirm Job Delete dialog box, click **Ok**.

The system deletes the selected download job.

## Viewing CRL download job

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Configuration > CRL Download**.  
The system displays the CRL Download Configuration page.
3. In **CRL Download Jobs**, select a job and click **View**.

The system displays the CRL Download Job Details page with all the download job details.

4. Click **Done** to return to the CRL Download Configuration page.

## CRL Download Configuration field descriptions

| Name                    | Description                                                                 |
|-------------------------|-----------------------------------------------------------------------------|
| <b>Select check box</b> | The option to select a download job.                                        |
| <b>Job Name</b>         | The name of the download job.                                               |
| <b>Last Run Date</b>    | Details of the last run download job, such as date, time, and time zone.    |
| <b>Last Run Status</b>  | The status of the last run download job, such as date, time, and time zone. |
| <b>Job State</b>        | The current state of the download job.                                      |
| <b>Frequency</b>        | The frequency of the download job.                                          |
| <b>Scheduled By</b>     | The name of the user who scheduled the download job.                        |

| Button        | Description                                                                             |
|---------------|-----------------------------------------------------------------------------------------|
| <b>Add</b>    | Displays the Schedule CRL Download page to create a new download job.                   |
| <b>Delete</b> | Displays the Confirm Job Delete dialog box to confirm the deletion of the download job. |
| <b>View</b>   | Displays the CRL Download Job Details page with all the details of the download job.    |

*Table continues...*

| Button        | Description                                                                                    |
|---------------|------------------------------------------------------------------------------------------------|
| Show All      | Shows all the download jobs.                                                                   |
| Select : All  | Selects all the download jobs.                                                                 |
| Select : None | Clears the selected download jobs.                                                             |
| Previous      | Displays the download jobs in the previous page. This button is unavailable on the first page. |
| Next          | Displays the download jobs in the next page. This button is unavailable on the last page.      |

| Icon                                                                              | Description                                         |
|-----------------------------------------------------------------------------------|-----------------------------------------------------|
|  | Refreshes the certificate information in the table. |

## CRL Download Job Details field descriptions

| Name                          | Description                                                                 |
|-------------------------------|-----------------------------------------------------------------------------|
| Job Name                      | The name of the download job.                                               |
| CRL Distribution Point        | The configured CRL distribution point for the download job.                 |
| Last Run Date                 | Details of the last run download job, such as date, time, and time zone.    |
| Last Run Status               | The status of the last run download job, such as date, time, and time zone. |
| Last Successful Download Date | The date when the download job successfully downloaded the CRL.             |

| Button | Description                                                                       |
|--------|-----------------------------------------------------------------------------------|
| Done   | Displays the CRL Download Configuration page listing all available download jobs. |

## Security Configuration field descriptions

### Global TLS Configuration

| Name                | Description                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Minimum TLS Version | The option to select the minimum TLS version to be supported.<br>For a military hardened system, only TLS version 1.2 is supported. |

### Revocation Configuration

| Name                              | Description                                                          |
|-----------------------------------|----------------------------------------------------------------------|
| Certificate Revocation Validation | The option to select the validation type for certificate revocation. |

*Table continues...*

| Name                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Revocation Type</b>            | <p>The option to select the certificate revocation type.</p> <p>This option cannot be changed if <b>Certificate Revocation Validation</b> is set to <b>NONE</b>.</p> <p> <b>Note:</b></p> <p>Only System Manager Release 7.1 and later supports <b>OCSP</b>. Other elements of Avaya Aura® Suite do not support <b>OCSP</b>. Therefore, it is recommended to not change the <b>Revocation Type</b> setting to <b>OCSP</b>.</p> |
| <b>Revocation Type Preference</b> | <p>The option to select the certificate revocation type.</p> <p>This option can be edited only if <b>Revocation Type</b> is set to <b>BOTH</b>.</p>                                                                                                                                                                                                                                                                                                                                                             |
| <b>Check method</b>               | <p>The Option to select the checking method for the certificate.</p> <p>This Option cannot be changed if <b>Certificate Revocation Validation</b> is set to <b>NONE</b>.</p>                                                                                                                                                                                                                                                                                                                                    |

## SMGR Cert based authentication

| Name                                     | Description                                                                                             |
|------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>For System Manager User Interface</b> | The option to enable or disable certificate-based authentication for the System Manager user interface. |
| <b>For Other TLS Ports</b>               | The option to enable or disable certificate-based authentication for other TLS ports.                   |

## Extended hostname validation

| Name                                | Description                                                   |
|-------------------------------------|---------------------------------------------------------------|
| <b>Extended Hostname Validation</b> | The option to enable or disable extended hostname validation. |

| Button        | Description                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------|
| <b>Commit</b> | Saves and commits any changes made in the security configuration with an automatic JBoss restart.   |
| <b>Cancel</b> | Cancels any changes made and reverts the security configuration settings to the last saved setting. |

## Deletion of expired certificates from System Manager

With Release 8.1.3, you can use the **Number of days after which system deletes expired certificates** field on the **Services > Configurations > Settings > SMGR > Trust Management** page to set the number of days to delete expired certificates from the system.



By default, System Manager runs **ExpiredCertificateRemovalJob** every week at 12 A.M. to check the expired certificates. If the certificate expires on or before the number of configured days, System Manager purges the expired certificates.

---

## Extended Hostname Validation

With the Extended Hostname Validation (EHV) feature, the system validates the host name or domain name of the server with the value in the **subject** or **subjectAltName** (SAN) field in the identity certificate for establishing the SSL connection.

---

## Enabling Extended Hostname Validation

### Procedure

1. On the System Manager web console, click **Services > Security > Configuration > Security Configuration**.
2. On the Security Configuration page, click **SMGR**.
3. In the Extended hostname validation section, select the **Extended Hostname Validation** check box.
4. Click **Commit**.

---

## External authentication

---

### External authentication

The External Identity Repositories Web page in System Manager contains a summary page for Authentication scheme and Authentication servers. You can configure the authentication scheme and the authentication servers for System Manager.

System Manager supports the following authentication authorities:

- Local users
- External RADIUS users
- External LDAP users
- External Security Assertion Markup Language (SAML) users

 **Note:**

- If you are using Microsoft Active Directory for external authentication with System Manager, the **userPrincipalName** attribute of the user in the external server must contain a valid value.
- If you are using the LDAP server other than Microsoft Active Directory for external authentication with System Manager, the **UID** attribute of the user in the external server must contain a valid value.

The authentication scheme policy determines the order in which you can use the authentication authorities. The supported order is as follows:

1. Local users (default)
2. External RADIUS users then local users
3. External LDAP users then local users
4. External Kerberos users, then local users
5. External LDAP users, then external RADIUS users, then local users
6. External RADIUS users, then external LDAP users, then local users
7. External KERBEROS users, then external multiple LDAP users, then local users

The authentication servers policy controls the settings for the external SAML, LDAP, RADIUS, and KERBEROS servers.

### Authentication scheme policy

System Manager supports the following authentication authorities:

- Local servers
- External RADIUS servers
- External LDAP servers (including Sun ONE or Microsoft active directory server)
- KERBEROS server
- SAML

---

## Editing the authentication scheme

### About this task

 **Note:**

The edit operation might reset the authentication scheme for the user. Ensure that the authentication scheme is correct.

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.

3. On the External Identity Repositories page, in the Authentication Scheme section, click **Edit**.
4. On the Authentication Scheme page, select the required authentication scheme.
5. Click **Save**.

---

## Provisioning of authentication servers

When the LDAP server is Microsoft Active Directory, the full name of the external user must be the same as the logon name that makes the cn attribute of the external users the same as the logon name.

The TCP port used for the external LDAP server and the UDP port used for the external RADIUS server must be open in the Linux iptables firewall, on both the primary security service, and the backup primary security service. To check the status of the iptables rules, use service iptables status.

---

## Provisioning the LDAP server

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, select **Provision First LDAP Server** and fill the required details in the fields.
5. **(Optional)** Select **Provision Second LDAP Server** and fill the required details in the fields.
6. Click **Save**.

### **Note:**

- Ensure that the Linux iptable firewall setting, on both the primary and backup security service, allows the TCP port as the source port.
- Clearing the **Provision First LDAP Server** check box clears all the data in the first and second provision LDAP server sections.

### Related links

[Authentication Servers field descriptions](#) on page 1243

---

## Provisioning the RADIUS server

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, select the Provision RADIUS Server option.
5. In the Provision RADIUS Server section, enter the relevant information.

You must create two records in the external RADIUS server with the same shared secret for both the primary security server and the backup security server IP address.

6. Click **Save**.

### **Note:**

Ensure that the Linux iptable firewall setting on both the primary and the backup security service has UDP port as the source port.

### Related links

[Authentication Servers field descriptions](#) on page 1243

---

## Provisioning the Kerberos server

### About this task

To use Kerberos authentication, configure System Manager with the required information for the Kerberos server.

### Before you begin

- If you use Firefox to gain access to System Manager, do the following:
  1. In the web browser, type `about:config`.
  2. Select the `network.negotiate-auth.trusted-uris` attribute.
  3. Right-click, select **Modify**, and add the URL of System Manager.
- Log on to System Manager with admin privileged credentials.

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.

4. On the Authentication Servers page, select the **Provision Kerberos Server** option.
5. In the **Provision Kerberos Server** section, enter the following information:
  - **DC Host Name (FQDN):** Type your FQDN in the format `machineName.domainName.com`. For example, `xyz.somecompany.com`.
  - **DC Computer Domain:** Type the domain name of the Kerberos server.
  - **Keytab File:** Click **Browse** and select the Kerberos server key file.
6. Click **Save**.

 **Important:**

When you log on to the Kerberos server using Single Sign-on (SSO), the system automatically authenticates you in the Domain Controller (DC) domain. Therefore, you cannot exit from UCM by using the **Logout** link. Close the web browser to exit the application.

#### Related links

[Authentication Servers field descriptions](#) on page 1243

## Provisioning user certificate authentication

### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, complete the information in the Provision User Certificate Authentication section.
5. Click **Save**.

## Authentication Servers field descriptions

### Provision First and Second LDAP Server

| Name                           | Description                                        |
|--------------------------------|----------------------------------------------------|
| <b>IP (or DNS)</b>             | The IP address or the DNS name of the LDAP server. |
| <b>TCP Port</b>                | The TCP port of the LDAP server.                   |
| <b>Base Distinguished Name</b> | The base distinguished name of the LDAP server.    |
| <b>SSL/TLS Mode</b>            | The connection type supported by the LDAP server.  |

*Table continues...*

| Name                                       | Description                                                                                                                                                                |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Is Active Directory</b>                 | The field to select if active directory does not support anonymous binding.                                                                                                |
| <b>Supports Anonymous Binding</b>          | The field to select if active directory supports anonymous binding.<br><b>Supports Anonymous Binding</b> field is inactive if <b>Is Active Directory</b> field is enabled. |
| <b>Distinguished Name for Root Binding</b> | The distinguished name for the root binding. For example, type <code>cn</code> for Users.                                                                                  |
| <b>Password for Root Binding</b>           | The password for the root binding in this field.<br>From Release 8.1.3, you can enter up to 256 characters for the LDAP server authentication.                             |

### Provision Radius Server

| Name                 | Description                                                  |
|----------------------|--------------------------------------------------------------|
| <b>IP (or DNS)</b>   | The IP address or the DNS name of the primary RADIUS server. |
| <b>UDP Port</b>      | The UDP port number of the primary RADIUS server.            |
| <b>Shared Secret</b> | The shared secret of the RADIUS server.                      |

### Provision Kerberos Server

| Name                       | Description                                                        |
|----------------------------|--------------------------------------------------------------------|
| <b>DC Host Name (FQDN)</b> | The FQDN in the following format: machineName.domainName.com/net/. |
| <b>DC Computer Domain</b>  | The domain name of the Kerberos server.                            |
| <b>Keytab File</b>         | The field to select the encrypted Kerberos server key.             |

### Provision SAML Remote Identity Provider

| Name                 | Description                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Entity ID</b>     | The entity ID of the provisioned SAML remote identity provider.<br>The text "-- not configured --" is displayed if a Remote Identity Provider is not configured.                              |
| <b>Metadata Type</b> | The method to query the metadata for Remote Identity Provider. The options are: <ul style="list-style-type: none"> <li>• URL. A valid HTTP URL.</li> <li>• File. A valid XML file.</li> </ul> |
| <b>Metadata Url</b>  | The valid HTTP URL for the metadata of Remote Identity Provider.<br>This field is disabled if the <b>File</b> option is selected in the <b>Metadata Type</b> field.                           |
| <b>Metadata File</b> | The valid XML file for the metadata of Remote Identity Provider.<br>This field is disabled if the <b>URL</b> option is selected in the <b>Metadata Type</b> field.                            |

*Table continues...*

| Name               | Description                                                                              |
|--------------------|------------------------------------------------------------------------------------------|
| <b>Choose File</b> | The field to select an XML file that contains the metadata for Remote Identity Provider. |

## Provision User Certificate Authentication

| Name                                           | Description                                                                                                                                                                                                                                        |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Certificate Purpose</b>                     | The purpose of the certification, such as Client Authentication.                                                                                                                                                                                   |
| <b>Certificate Field Name to get User Name</b> | The fields that can be used to retrieve the username from the certificate.<br>The left section contains the fields that can be read from the certificate.<br>The right section contains the fields that the system will read from the certificate. |

| Button          | Description                                                |
|-----------------|------------------------------------------------------------|
| <b>Remove</b>   | Removes the selected client purpose.                       |
| <b>Add</b>      | Adds the typed client purpose.                             |
| <b>&gt;&gt;</b> | Moves the selected certificate field to the right pane.    |
| <b>&lt;&lt;</b> | Moves the selected certificate field to the left pane.     |
| <b>Up</b>       | Increments the priority of the selected certificate field. |
| <b>Down</b>     | Decrements the priority of the selected certificate field. |

| Button        | Description                                             |
|---------------|---------------------------------------------------------|
| <b>Save</b>   | Saves your settings on the Authentication Servers page. |
| <b>Cancel</b> | Cancels your action and takes you to the earlier page.  |

---

## SAML authentication

### SAML authentication

For enterprise level Single Sign On, System Manager provides Security Assertion Markup Language (SAML) authentication.

### SAML protocol

SAML is an XML-based open standard used for exchanging authentication and authorization data between an identity provider, a producer of assertions, and a service provider, a consumer of assertions. SAML product belongs to the OASIS Security Services Technical Committee.

SAML protocol does not provide rules for determining the identity and access levels of a subject. The SAML protocol shares the authentication and authorization information of an identity between the issuer of the information, called as the identity provider and the relying party or the consumer of the information, called as the service provider.

## Key components of SAML protocol

### Assertions

Assertions are the packets of security information transferred from the Identity Provider to the Service Provider. The following are three different types of statements in an Assertion:

- Authentication Statements
- Attribute Statements
- Authorization Decision Statements

Assertions that the Identity Provider issues have a validity period beyond which the service provider must reject the information. SAML uses Authentication Statement to validate identity of the user.

### Protocols

SAML protocol provides rules on how SAML elements must be packaged in SAML request and response messages. The following are some of the key SAML protocols:

- Authentication Request Protocol
- Artifact Resolution Protocol
- Assertion Query and Request Protocol

Assertions that the Identity Provider issues have a validity period beyond which the service provider must reject the information. SAML/System Manager uses Authentication Statement to validate user's identity.

### Bindings

SAML binding refers to the mapping of a SAML message to a communication protocol or method. The following are some of the main SAML binding mechanisms:

- HTTP POST
- HTTP Redirect
- HTTP Artifact
- SOAP

### Profiles

SAML profile describes how various SAML messages, protocols, and bindings can combine together to achieve a particular use case.

Web Browser SSO Profile is the widely used SAML Profile. Web Browser SSO Profile provides the use case to achieve Single Sign On from a Web browser when you gain access to a protected resource on the service provider.

## SAML implementation in System Manager

System Manager uses SAML implementation version 2.0 of OpenAM Release 9.5.4 to provide SAML based authentication with external/remote Identity Providers. System Manager functions as



a Service Provider, consumer of assertions. You can configure CA Siteminder or a similar solution as a Remote Identity Provider, the producer of assertions.

System Manager uses Web Browser Single Sign On profile of SAML authentication. In System Manager, authentication using SAML differs from other external authentication methods such as remote LDAP and RADIUS in the following ways:

- You require a special URL to invoke SAML based authentication. You can bookmark a URL as <https://smgr.ca.avaya.com/?performssso=saml>.

The system subjects:

- Any incoming HTTP request to System Manager with a request parameter `performssso` set to `saml` to SAML based authentication.
- All other URLs to existing authentication handling and redirects an unauthenticated request to the login screen of System Manager.
- System Manager does not provide its own login screen for SAML authentication. The system redirects an unauthenticated user to the login screen of Remote Identity Provider (R-IDP). On successful authentication, the system redirects you to System Manager.

## Salient features of SAML implementation in System Manager

- R-IDP and System Manager always communicates through HTTPS.
- System Manager and identity provider communicates through HTTP-POST binding.
- SAML implementation module does not validate CRL. However, SSL communication fails with a certificate that is revoked since, SSL setup in System Manager jboss container ensures CRL validation.
- The system rejects expired Assertions.

## Guidelines for SAML authentication in System Manager

- You can use the NameID of a subject in an Assertion as the login ID to create a user account for the subject in System Manager. If the system encrypts the NameID, R-IDP must include the attributes of authenticated subject such as uid and email. in the Assertion. The system uses the attributes to create a user account in System Manager. If the Assertion does not contain attributes, the R-IDP must act as an Attribute Authority. In System Manager, you require an account for RBAC.
- Assertions must be signed and not encrypted.
- The system uses assertions from trusted sources only. An administrator must setup SSL trust between System Manager and R-IDP by adding the CA certificate of R-IDP's Web server certificate into the CA truststore in System Manager.
- Condition statement in an Assertion can have multiple AudienceRestriction statements. The condition statement must have SAML entity ID of System Manager as one of the AudienceRestriction.

## Configuring System Manager for SAML authentication

### Configuring Hosted Service Provider on System Manager

#### About this task

The system automatically configures System Manager as Hosted Service Provider during the installation of System Manager and upgrade of System Manager from Release 6.2.

However, you can modify the configuration using the following procedure.

As an administrator, you can enable or disable SAML authentication in System Manager from the SAML Configuration page.

#### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication > SAML Configuration**.
3. Click **Edit**.
4. On the SAML Hosted Service Provider page, perform the following:
  - a. Perform one of the following:
    - Select the **NameID as UserID** check box.
    - In the **Attribute Used as UserID** field, enter the name of the attribute that you want to use as the login ID of the user in System Manager.

#### SAML Configuration

Customize configuration on the Hosted Service Provider for external SAML authentication and on the Hosted Identity Provider for SAML authentication in the domain.

Host Configuration for External Authentication Enable Edit...

Entity ID: https://host1234.smgravaya.com:443/securityserver  
 Meta Alias Name: /sp  
 NameID as UserID: false  
 Attribute Used as UserID: uid  
 Mapped Attributes: mail=mail  
                       EmailAddress=mail  
                       UserID=uid  
                       uid=uid

[Download Hosted Service Provider metadata...](#)

- b. In the **Mapped Attributes** field, enter an attribute that you require to map between R-IDP and H-SP for a user.
  - c. Click **Save**.

### Configuring Remote Identity Provider

#### Procedure

1. Download the XML metadata from the Identity Provider:
  - a. Download the metadata in XML format that contains the service descriptor information of Remote Identity Provider (R-IDP) from the R-IDP server or using a valid HTTP URL that R-IDP provides.

For example, if OpenAM is configured as the R-IDP, download the metadata from <https://my-openam.ca.avaya.com/opensso/saml2/jsp/exportmetadata.jsp>.

- b. Save the data in an XML file on the file system or save the URL that points to the metadata.
2. Setup SSL trust between R-IDP and System Manager for successful communication of SAML messages using the following steps:
  - a. On System Manager Web Console, click **Services > Inventory**.
  - b. In the left navigation pane, click **Manage Elements** and add the CA certificate of R-IDP Web server certificate to System Manager truststore using the instructions outlined in Adding trusted certificates.
3. Add Remote Identity Provider:
4. Click **Save**.

On successful configuration of R-IDP, the system automatically enables the SAML authentication. An administrator can disable or enable the SAML authentication using the **Provision SAML Remote Identity Provider** check box.

## Related links

[Adding trusted certificates](#) on page 1184

[Provisioning Remote Identity Provider](#) on page 1249

## Provisioning Remote Identity Provider Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **User Services > External Authentication**.
3. On the External Identity Repositories page, click **Configure** in the Authentication Servers section.
4. On the Authentication Servers page, select the **Provision SAML Remote Identity Provider** check box and get the metadata of R-IDP using one of the following:
  - Through a valid HTTP URL.
  - Using a valid XML file.

☐ Provision SAML Remote Identity Provider

Entity ID: -- not configured --

Metadata Type: ☒ URL ☐ File

Metadata Url:

Metadata File:  No file chosen

5. Click **Save**.

If R-IDP is successfully configured, the system automatically enables SAML authentication. An administrator can disable or enable SAML authentication using the **Provision SAML Remote Identity Provider** check box.

#### Related links

[Authentication Servers field descriptions](#) on page 1243

---

## Active sessions

---

### Viewing active sessions

#### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Active Sessions**.
3. On the Active Sessions page, the sessions are sorted in the **User ID** column.

---

### Terminating Single Sign-On sessions

#### About this task

Use this functionality to terminate selected Single Sign-On (SSO) sessions.

#### Procedure

1. On the System Manager web console, click **Users > Administrators**.
2. In the navigation pane, click **Security > Active Sessions**.
3. On the Active Sessions page, select the check box beside the required sessions to terminate.
4. Click **Terminate**.

The system deletes the selected sessions from the current sessions table. Administrators with terminated sessions are required to log on again.

---

# Regenerating data protection keys

---

## Regenerating symmetric keys for System Manager

### About this task

Use this procedure to execute the utility to regenerate data protection keys. System Manager administrator must execute the utility manually when one or more of the following conditions are met:

- Commercial grade hardening is enabled in System Manager.
- Sensitive data, such as user or communication profile passwords, are suspected to be compromised.
- The older data encryption keys must be replaced.

### Before you begin

- Create a data backup of System Manager before running this utility.
- On Geographic Redundancy-enabled System Manager, disable replication before executing this utility.

For more information, see “Disabling the Geographic Redundancy replication”.

- Stop the System Manager JBoss service.

### \* Note:

The utility takes longer when a large amount of data is present on System Manager. Therefore, Avaya recommends that you run this utility during the System Manager maintenance window.

### Procedure

1. Log in to the System Manager command line interface.
2. Type `cd $MGMT_HOME/securestore`, and press `Enter`.
3. Type `sudo $MGMT_HOME/securestore/migrateORRegenSecureStores.sh 3600`, and press `Enter`.
4. At the prompt, type one of the following and press `Enter`:
  - 1 to run the utility for all domains
  - 2 to run the utility for specific domains
  - 3 to exit the utility

5. To run the utility for specific domains, enter the domain name and press `Enter`.

The system executes the utility as a background process. Thus, if the SSH session is terminated, the utility execution is not affected.

6. To view the result, type `vim $AVAYA_LOG/migrateOrRegenSecureStore.log` and press `Enter`.

**Related links**

[Disabling the Geographic Redundancy replication](#) on page 112

---

## Regenerating asymmetric keys for System Manager

**About this task**

Use this procedure to execute the utility to regenerate asymmetric data protection keys. System Manager administrator must run this shell-based utility in one or more of the following conditions:

- One or more asymmetric keys are suspected to be compromised.
- **Key Management Properties** sends a trap notification.
- Asymmetric keys are outdated and need to be regenerated.

**Before you begin**

- Stop the System Manager JBoss service.

 **Note:**

The utility takes more time to run when a large amount of data is present on System Manager. Therefore, Avaya recommends that you run this utility during the System Manager maintenance window.

**Procedure**

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `cd /opt/vsp`, and press `Enter`.
3. Type `sh regenerateSSHKeys.sh`, and press `Enter`.

**Next steps**

1. Start the System Manager JBoss service.
2. Using the Solution Deployment Manager client, reestablish connection for all client elements.

---

## Regenerating asymmetric keys for geographic redundancy-enabled System Manager

**About this task**

Use this procedure to execute the utility to regenerate asymmetric data protection keys. System Manager administrator must run this shell-based utility in one or more of the following conditions:

- One or more asymmetric keys are suspected to be compromised.
- **Key Management Properties** sends a trap notification.
- Asymmetric keys are outdated and need to be regenerated.

## Before you begin

- Disable geographic redundancy replication.  
For more information, see “Disabling the Geographic Redundancy replication”.
- Convert the primary System Manager server to a standalone server.  
For more information, see “Converting the primary System Manager server to the standalone server”.
- Stop the System Manager JBoss service.

### **Note:**

The utility takes more time to run when a large amount of data is present on System Manager. Therefore, Avaya recommends that you run this utility during the System Manager maintenance window.

## Procedure

1. Log in to the System Manager command line interface.
2. Type `su - root`, and press `Enter`.
3. Provide the root password, and press `Enter`.
4. Type `cd /opt/vsp`, and press `Enter`.
5. Type `sh regenerateSSHKeys.sh`, and press `Enter`.
6. Start the System Manager JBoss service.

## Next steps

1. Configure System Manager to enable geographic redundancy.  
For more information, see “Enabling the Geographic Redundancy replication”.
2. Using the Solution Deployment Manager client, reestablish connection for all client elements.

## Related links

[Disabling the Geographic Redundancy replication](#) on page 112

[Converting the primary System Manager server to the standalone server](#) on page 119

[Enabling the Geographic Redundancy replication](#) on page 111

[Re-establishing trust for Solution Deployment Manager elements](#) on page 1356

# Chapter 21: Managing tenants

---

## Multi Tenancy

Tenant is a client organization that uses Team Engagement OnAvaya Aura – Unified Communications as a Service (UCaaS) (Avaya CE for UC) or Private Cloud in a shared, hosted environment. The tenant purchases the services on a pay-per-usage basis from the service provider. The tenant can contain a list of sites.

### Multi Tenancy

By default, the Multi Tenancy feature is disabled. You must enable the Multi Tenancy feature. After you enable the Multi Tenancy feature, you cannot disable the feature.

- **Multi Tenancy elements:** Communication Manager, Avaya Messaging, and Session Manager
- **Single Tenancy elements:** UCM Applications and Messaging

#### **Note:**

The elements that do not support any type of Multi Tenancy must not be configured for the User Provisioning Rule that the user wants to add to the tenant site because the system validates each User Provisioning Rule against the elements that are available in the Tenant site. In case the User Provisioning Rule contains elements, which do not support Single or Multi Tenancy, then the administrator cannot add the User Provisioning Rule to the tenant site.

The Service Provider Administrator and System Administrator can assign an element that supports:

- Multi Tenancy to more than one tenants. For example, Communication Manager.
- Single tenancy to only one tenant. For example, Messaging and IP Office.

### Tenant Management

To support Multi Tenancy, System Manager provides Tenant Management.

System Manager supports three levels of organization hierarchy for tenant management. The following lists the default names of the levels:

- Level 1: Site
- Level 2: Department
- Level 3: Team

The administrator can modify the default level names. The organization hierarchy levels, level 2 and level 3, are optional.



## Tenant Management on Out of Band Management-enabled System Manager

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

For more information about configuring Multi Tenancy on Out of Band Management-enabled System Manager, see *Deploying Avaya Aura® System Manager*.

### Related links

[Tenant Management web console](#) on page 57

---

## Enabling Multi Tenancy

### Before you begin

Log on to the System Manager web console as Service Provider Administrator or Tenant Administrator.

### About this task

To perform tenant-related administration, you must enable the Multi Tenancy feature on System Manager web console.

After you enable the Multi Tenancy feature, you cannot disable the feature. To disable the Multi Tenancy feature, you must reinstall System Manager. By default, the system disables the Multi Tenancy feature.

### Procedure

1. On the System Manager web console, click **Services > Configurations**.
2. In the navigation pane, click **Settings > SMGR**.
3. On the View Profile:SMGR page, click **Edit**.

The system displays the Edit Profile:SMGR page.

4. In Multi Tenancy Properties, set **Multi Tenancy Status** to `true`.
5. Click **Commit**.
6. Log off from System Manager, and log on to System Manager again.

The administrator can now manage tenants from the **Services > Tenant Management** page on the System Manager web console.

---

## Creating a tenant

### Before you begin

- Log on to the System Manager web console as Service Provider Administrator or Tenant Administrator.
- Enable the Multi Tenancy feature.
- After you enable Multi Tenancy, log off and log on to the System Manager web console again.

### About this task

Use the procedure to create a tenant, assign a tenant administrator to the tenant, create tenant organization, and assign elements and user provisioning rule.

You can create one or more tenants.

System Manager supports maximum 250 tenant partitions as part of System Manager Multi Tenant Management.

### Procedure

1. On the System Manager web console, click **Services > Tenant Management**.
2. On the Tenant Management page, click **New Tenant**.  
The system displays the Create Tenant page.
3. On the Tenant Details tab, provide the details for the tenant.  
For more information, see Create Tenant field descriptions.
4. On the Administrators tab, in the Assigned Admin Users section, perform the following:
  - a. Click **New**.
  - b. In the Create Admin User area, provide the details of the administrator that you want to assign to the tenant.
  - c. Click **Commit**.
5. **(Optional)** On the Organization Hierarchy tab, in the Organization level names section, change the names for **Level 1**, **Level 2**, and **Level 3**.  
Level 2 and Level 3 are optional.
6. To view the new tenant node, click **Update Hierarchy**.  
If you do not click **Update Hierarchy**, the page does not display the new tenant that you created. Therefore, you cannot add a site to this tenant.
7. Perform the following to add a site or level 1 organization to the tenant:
  - a. In the Tenant Hierarchy section, select the tenant that you created and click **Add**.
  - b. Provide the following details for the site:
    - **Site Details:** Details of the site. For more information, see Create Tenant field descriptions.

- **Elements:** Perform the following:
- To assign an element to the site, click the plus sign (+) in the Available Elements section.

Click **X** to unassign an element if required. You can assign more than one element to a site. The Selected Elements section displays the elements that you assign to the site. Provide the tenant number or tenant ID and the location number for the element.

**New Tenant**

Search ...

- Audi
  - McDonalds
    - Pune Centre**
      - TenantBMW
      - TenantFord

**Pune Centre Details** \* **Elements** User Provisioning Rule

**Selected Elements**

1 Item

| Name        | Type | Tenant Number | Location Number |
|-------------|------|---------------|-----------------|
| X CMElement | CM   | 12            |                 |

**Available Elements**

0 Items Filter: Enable

| Name       | Type |
|------------|------|
| No Records |      |

Commit Cancel

**\* Note:**

The Communication Manager element that you select in the Elements tab and the User Provisioning Rule tab must be the same. If you select a different Communication Manager element, the tenant creation fails.

- To assign permissions to the tenant administrator, click the element, select the permissions on the Permission Mappings page, and click **Commit**.

For more information, see the “Managing roles”.

**\* Note:**

For Communication Manager, do not provide permissions for Audit, Element Cut Through, and Synchronization functions.

- **User Provisioning Rule:** Click the plus sign (+) in the Available User Provisioning Rules section to assign a rule to the site. Click **X** to unassign a user provisioning rule.

- Click **Update Hierarchy** to view the new site in the tenant organization.

The system displays the site that you added to the tenant.

If you do not click **Update Hierarchy**, the system does not display the new site that you created. Therefore, you cannot add a department to this site.

**\* Note:**

Add at least one site for the tenant.

- Repeat Step a through Step c to add more than one site for the tenant.
- (Optional) Perform the following to add a department or level 2 organization to the site:
    - In the Tenant Hierarchy section, select the site, and click **Add**.
    - Provide the details for the department.
    - Click **Update Hierarchy** to view the new department in the tenant organization.

If you do not click **Update Hierarchy**, the system does not display the new department that you created. Therefore, you cannot add a team to this department.

- d. Repeat Step a through Step c to add more than one department for the site.
  9. **(Optional)** Perform the following to add a team or level 3 organization to the department:
    - a. In the Tenant Hierarchy section, select the department, and click **Add**.
    - b. Provide the details for the team.
    - c. Click **Update Hierarchy** to view the new team in the tenant organization.
 

If you do not click **Update Hierarchy**, the system does not display the new team that you created.
    - d. Repeat Step a through Step c to add more than one team for the department.
  10. Click **Commit**.
- The system displays the tenant organization on the Tenant Management page.
11. Repeat Step 2 through Step 9 to create more than one tenant.

#### Related links

[Adding a custom tenant administrator role](#) on page 189

[Enabling Multi Tenancy](#) on page 1255

[Unassigning the tenant administrator](#) on page 1260

[Tenant Management field descriptions](#) on page 1267

[Create Tenant field descriptions](#) on page 1267

---

## Assigning the tenant administrator to the tenant

### Before you begin

- Log on to the System Manager web console as the Cloud Service Provider administrator.
- Enable the Multi Tenancy feature.

### Procedure

1. On the System Manager web console, click **Services > Tenant Management**.
2. On the Tenant Management page, select a tenant in the left pane, and click the **Administrators** tab.
3. In the **Assigned Admin Users** section, perform one of the following steps:
  - Click **Edit** or **Search** and select the administrator that you must assign to this tenant.
  - Perform the following:
    - a. Click **New**.
    - b. In the **Create Admin User** area, provide the details of the administrator that you must assign to the tenant.

- c. Click **Commit**.

The system assigns the tenant administrator to the tenant.

---

## Unassigning the tenant administrator

### Before you begin

- Log on to the System Manager web console as the Service Provider Administrator.
- Enable the Multi Tenancy feature.
- Create the tenant.

### Procedure

1. On the System Manager web console, click **Services > Tenant Management**.
2. On the Tenant Management page, select the tenant in the left pane, and click the **Administrators** tab.
3. In the **Assigned Admin Users** section, click **Edit** or **Search**, and select the administrator that you must unassign.
4. Click **Unassign**.
5. Click **Commit**.

The system removes the association of the tenant administrator with the tenant.

### Related links

[Tenant Management field descriptions](#) on page 1267

[Create Tenant field descriptions](#) on page 1267

---

## Viewing the tenant

### Before you begin

- Log on to the System Manager web console.
- Enable the Multi Tenancy feature.
- Create a tenant.

### Procedure

1. On the System Manager web console, click **Services > Tenant Management**.
2. From the tenant organization, click the tenant, site, department, or team that you want to view.
3. View the details of the tenant, site, department, or team.

**Related links**

[Tenant Management field descriptions](#) on page 1267

[Create Tenant field descriptions](#) on page 1267

---

## Modifying the tenant

**Before you begin**

- Log on to the System Manager web console as Service Provider Administrator or Tenant Administrator.
- Enable the Multi Tenancy feature.

**About this task**

Use the procedure to modify the following:

- The tenant, organization hierarchy, and tenant administrator details.
- The assignment of elements, user provisioning rule, and resource permissions to the site.

**Procedure**

1. On the System Manager web console, click **Services > Tenant Management**.
2. On the Tenant Management page, select the tenant, site, department, or team that you must modify.
3. Click **Edit**.
4. Modify the following information as appropriate:
  - Tenant details, tenant administrator, and organization hierarchy labels
  - Site details, assignment of elements, user provisioning rule, and permissions to the site
  - Department details
  - Team details

For information, see Create Tenant field descriptions.

5. Click **Commit**.

**Related links**

[Tenant Management field descriptions](#) on page 1267

[Create Tenant field descriptions](#) on page 1267

---

## Deleting a tenant

The Service Provider Administrator can delete the tenant and the tenant organization hierarchy.

## Before you begin

- Log on to System Manager Web Console as Service Provider Administrator.
- Enable the Multi Tenancy feature.
- Delete all users associated with the tenant.

## Procedure

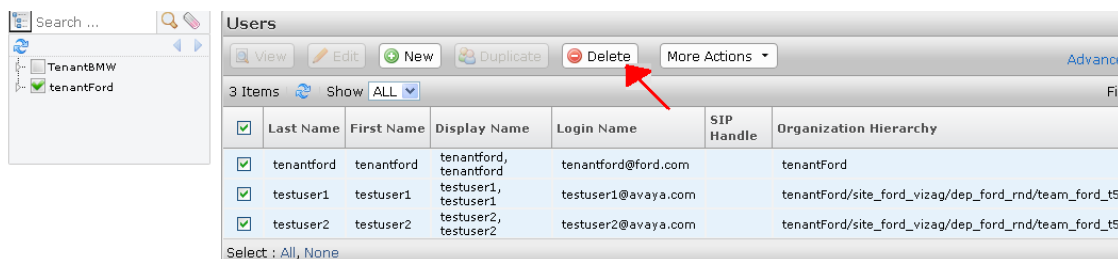
1. On the System Manager web console, click **Services > Tenant Management**.
2. On the Tenant Management page, select the tenant that you must delete.
3. Click Delete.

If any users associated with the tenant exist, the system displays a message to delete all users.

4. **(Optional)** Perform the following steps to delete users associated with the tenant:

- a. On the User Management page, in the tenant organization, select a tenant.

The system displays the users associated with this tenant on the right pane. You can search for a tenant if you cannot view the tenant in the left pane.



- b. Select the users, and click **Delete**.
- c. On the User Delete Confirmation page, click **Delete**.

The system deletes the users that are associated with the tenant.

5. On the Organization Unit Delete Confirmation page, click **Delete**.

The system deletes the tenant, tenant administrator, and all roles created for the tenant, sites, departments, and organization for the tenant.

## Related links

[Tenant Management field descriptions](#) on page 1267

[Create Tenant field descriptions](#) on page 1267



---

## Multi Tenancy for Avaya SIP AST endpoints

During the search for enterprise users that must be added as contacts, Avaya SIP AST endpoints retrieve the enterprise users from:

- The tenant partition to which the enterprise user who started the search belongs
- The enterprise users in the default tenant partition
- All public contacts

---

## Multi Tenancy for Communication Manager objects

With the Multi Tenancy feature, Communication Manager provides telecommunication services to multiple, independent groups of users through a single Communication Manager server. Each tenant appears to have a dedicated Communication Manager server, though in reality, the tenants share the same Communication Manager server.

As an administrator, you can gain access to one or more tenant partitions in System Manager, and you can administer tenant numbers for several Communication Manager objects. You can segregate tenants through tenant numbers. The following Communication Manager objects support Multi Tenancy:

- Agents
- Announcements
- VDN
- Endpoints
- Term Extension Group
- Trunk Group
- Hunt Group

When a user is added to a tenant, the **Tenant Number** field is autopopulated for these Communication Manager objects.

The Communication Manager Objects page displays specific Communication Manager objects based on the tenant permissions and the Communication Manager permissions that you specify.

 **Note:**

For a Communication Manager instance, do not assign the same tenant number for more than one tenant.

After the tenant administrator selects the site and the tenant from the Tenant Management web console, the Communication Manager Objects page displays the tenant and site combination. Depending on the tenant and site a user selects, the tenant range and tenant permissions take effect.

## Multi Tenancy and tenant partitioning in Communication Manager

The native tenant partitioning feature of Communication Manager provides multiple services to independent groups of users through a single Communication Manager server. Communication Manager also offers the following features:

- Segmenting call processing and feature processing by the Inter-Tenant Communications Control (ITCC) feature
- Tenant management of users and system administrators through System Manager

With System Manager Inter-tenant Communication Control (ITCC), Communication Manager can segregate features for each customer. System Manager tenants are shared across multiple adopters. Communication Manager is one of the adopters. Based on the roles and permissions assigned on the Communication Manager instances in a tenant, the Communication Manager objects are segregated for the tenant.

---

## Notes on Multi Tenancy for Communication Manager

### Scheduling jobs with Multi Tenancy

When the Multi Tenancy feature is enabled you cannot schedule the following operations:

- Clear amw
- Delete station
- Delete agent
- Delete announcement
- Backing up announcements
- Backing up all announcements
- Restoring announcements
- Restoring all announcements
- Moving announcements
- Broadcasting announcements
- Bulk operations including adding stations in bulk, deleting stations in bulk, adding agents in bulk, deleting agents in bulk, editing agents in bulk
- Global endpoint change

Tenant administrators cannot delete Communication Manager objects in System Manager. To assign delete permissions to a tenant administrator, the Service Provider Administrator must provide delete and scheduler permissions to the tenant administrator.

This will not impact the current implementation of Element Cut Through, notify sync, and adding Off PBX entries for a SIP station.

### User Provisioning Rule and Multi Tenancy

When you assign a user provisioning rule to a tenant, the same Communication Manager element must be present in User Provisioning Rule and Elements tabs. If the Communication Manager

element that you selected is available in the User Provisioning Rule tab but unavailable in the Elements tab, the tenant creation fails.

When you create a new tenant, the system validates the tenant number based on the Communication Manager that you selected. Depending on the tenant configuration in the Communication Manager you selected, you can choose a tenant number between 1 to 100 or 1 to 250.

## User Management and Multi Tenancy

When you enable the Multi Tenancy feature, and you choose the tenant and site for a user in User Management, the system displays Communication Manager **System** in the endpoint agent communication profile sections based on the tenant and site values you selected in the Identity tab. The User Management values override the values selected on the **Multi Tenancy** dashboard.

The system displays the available extensions in the endpoint, agent communication profile sections according to the tenant and Communication Manager permissions.

## Field level permissions and Multi Tenancy

Apart from the tenant permissions, object-level and field-level permissions are also valid for the tenant hierarchies. For example, admin A with access to Tenant Partition 1 can modify hunt-group 12 in Tenant Partition 1, but admin A cannot assign a station in Tenant Partition 2 to that hunt group.

The object and field-level permissions are valid for the following objects:

| Communication Manager object | Fields                                                                                                                       |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Hunt Group                   | Group Number Range<br>Group Extension<br>Member Extensions<br>Night Attendant Extension                                      |
| Agents                       | Agent Login ID<br>Coverage Path<br>Port Extension<br>COR<br>Tenant Number                                                    |
| VDN                          | Extension<br>COR<br>Tenant Number<br>VDN of Origin Annc Extension<br>Return Destination<br>Conference Controller for Meet-me |

*Table continues...*

| Communication Manager object | Fields                                                                                                                       |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Endpoint                     | COR<br>Emergency Location Extension<br>Message Lamp Extension<br>Tenant Number<br>Media Complex Extension<br>Hunt-to Station |
| Terminating Extension Group  | Group Extension<br>COR<br>Tenant Number<br>4 Extension fields                                                                |
| Trunk Group                  | COR<br>Tenant Number<br>Incoming Destination<br>Night Service Extension<br>List of Trunk Group Data                          |

- Do not provide Element Cut-Through access for a tenant administrator, because the administrator can bypass the tenant restrictions.
- In the Tenant Management web console, when the tenant administrator assigns a single number or a range in the **Tenant Number** field, the Communication Manager that the administrator selects is associated with the tenants.

The **Tenant Number** field is autopopulated for the Communication Manager objects that you create through Communication Manager. In the **Tenant Number** field, you can specify only the values or range that you configured in System Manager. If you specify a range, the system uses the smallest value in the tenant range. This scenario is also valid when you create Communication Manager objects such as endpoints or agents using User Management or Directory Synchronization.

- When you create tenants, if you specify the location, then you can enter only valid values. Location can be a single number, a range, or blank. When you enable multi-location field in System-Parameters customer-options, the available values for the **Location Number** field are 1 to 250 for Communication Manager 6.0 and 6.2, and 1 to 2000 for Communication Manager 6.3 and later. You must type `blank` or leave the **Location** field blank to choose blank as a value for tenant objects. For example, to specify blank and the range 1 to 10, you must type `blank, 1:10` in the **Location** field.
- When you change or select a template, the **Tenant Number** in the template takes precedence over the smallest, default tenant value. This scenario is valid only if the tenant number present in the template is within the valid tenant range. Otherwise, the system uses the smallest value in the specified tenant range. The value in the **Location** field specified in the template also takes precedence over the default value. The system validates against incorrect and out of range values.

## Tenant Management field descriptions

### Tenant Hierarchy

| Button            | Description                                                                                                                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>New Tenant</b> | Displays the Create Tenant page where you can create new tenants and the organization hierarchy.                                                                                                                                                  |
| <b>Add</b>        | Displays the following tabs when you select a tenant and click <b>Add</b> . <ul style="list-style-type: none"> <li>• <b>Level 1 Details</b> or <b>Site Details</b></li> <li>• <b>Elements</b></li> <li>• <b>User Provisioning Rule</b></li> </ul> |
|                   | Displays the <b>Department Details</b> section when you select the level 1 or site, and click <b>Add</b> .                                                                                                                                        |
|                   | Displays the <b>Team Details</b> section when you select the level 2 or department, and click <b>Add</b> .                                                                                                                                        |

| Icon                                                                              | Name   | Description                                 |
|-----------------------------------------------------------------------------------|--------|---------------------------------------------|
|  | Search | Searches for the tenant that you specified. |
|  | Clear  | Clears the search text.                     |

## Create Tenant field descriptions

The system displays the Create Tenant page when you click **New Tenant** or select a tenant organization from the tree.

 **Note:**

Fields marked with an asterisk are mandatory.

### Tenant Details

| Name                   | Description                                                                                                                                                                                                                                                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>            | The name or unique identifier of the tenant.                                                                                                                                                                                                                                                     |
| <b>Contact ID</b>      | The contact ID of the tenant.                                                                                                                                                                                                                                                                    |
| <b>Max no of users</b> | <p>The maximum number of users that an administrator can associate with this tenant.</p> <p>This number does not include admin users who can manage this tenant but are not associated with this tenant.</p> <p>You can administer 10–250000 end users in System Manager. The default is 10.</p> |
| <b>Description</b>     | A brief description of the tenant.                                                                                                                                                                                                                                                               |

## Administrators

The Assigned Admin Users section displays the fields in the Create Admin User area when you click **New**.

| Name                    | Description                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>First Name</b>       | The first name of the administrator.                                                                                          |
| <b>Last Name</b>        | The last name of the administrator.                                                                                           |
| <b>Login</b>            | The login name of the administrator.<br>The login name must be a fully qualified domain name. For example, jmiller@avaya.com. |
| <b>Password</b>         | The password to log on to the System Manager web console.                                                                     |
| <b>Confirm Password</b> | The password that you must re-enter for confirmation.                                                                         |

| Button          | Description                                                                |
|-----------------|----------------------------------------------------------------------------|
| <b>New</b>      | Creates a new tenant administrator with the details that you provide.      |
| <b>Search</b>   | Searches for the administrator using the search criteria that you provide. |
| <b>Unassign</b> | Removes the administrator that you selected.                               |
| <b>Commit</b>   | Saves the administrator details that you provided.                         |
| <b>Cancel</b>   | Cancels the operation.                                                     |

## Organization Hierarchy

The page displays the fields in the Organization Level Names area.

| Field   | Description                                  |            |                    |
|---------|----------------------------------------------|------------|--------------------|
| Level 1 | The name for level 1.                        |            |                    |
|         | Organization level                           | Default    | Example            |
|         | Level 1                                      | Site       | Hyderabad          |
|         | Level 2                                      | Department | Loans Division     |
|         | Level 3                                      | Team       | Customer Relations |
| Level 2 | The name for level 2. The field is optional. |            |                    |
| Level 3 | The name for level 3. The field is optional. |            |                    |

| Button                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Update Hierarchy</b> | <p>The system performs the following:</p> <ul style="list-style-type: none"> <li>• Refreshes the page with the details that you provided during the creation of the tenant, site, department, and team.</li> <li>• Displays the tenant node that you created.</li> <li>• Displays the level 1 or site that you created.</li> <li>• Displays the level 2 or department that you created.</li> <li>• Displays the level 3 or team.</li> </ul> <p> <b>Note:</b></p> <p>The system displays the newly created organizational unit only when you click <b>Update Hierarchy</b>.</p> |
| <b>Commit</b>           | Saves the changes you made to the tenant, site, department, or team, and displays the Tenant Management page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Cancel</b>           | Cancels the current operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Level 1 Details or Site Details

The system displays the Level 1 Details or Site Details, Elements, and User Provisioning Rule tabs only when you select a tenant, and click **Add**.

| Name               | Description                                           |
|--------------------|-------------------------------------------------------|
| <b>Name</b>        | The name of the level 1 hierarchy or site.            |
| <b>Address</b>     | The address of the level 1 hierarchy or site.         |
| <b>Description</b> | A brief description of the level 1 hierarchy or site. |

### Elements

| Name                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Selected Elements</b>                                                            | <p>The elements that you can assign to the level 1 hierarchy or site.</p> <p>The system adds the elements to the section from the <b>Available Elements</b> section when you click the plus sign (+).</p> <p> <b>Note:</b></p> <p>The element that you select in the <b>Elements</b> tab and the <b>User Provisioning Rule</b> tab must be the same. If you select a different element, the tenant creation fails.</p> |
|  | <p>Unassigns the element from the level 1 hierarchy or site.</p> <p>The system displays the element in the <b>Available Elements</b> section.</p>                                                                                                                                                                                                                                                                                                                                                         |
| <b>Name</b>                                                                         | The name of the element.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Type</b>                                                                         | The element type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

*Table continues...*

| Name                      | Description                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tenant No.</b>         | The tenant unique identifier.<br><br>The <b>Tenant No.</b> and <b>Location No.</b> must be created in the element before you associate the numbers with the tenant. For information, see the documentation for the appropriate element. |
| <b>Location No.</b>       | The site that contains elements and other network element resources. For example, Communication Manager, Session Manager, endpoints, and other resources.                                                                               |
| <b>Available Elements</b> |                                                                                                                                                                                                                                         |
| +                         | Click to assign the element to the site.                                                                                                                                                                                                |
| <b>Name</b>               | The name of the element.                                                                                                                                                                                                                |
| <b>Type</b>               | The element type.                                                                                                                                                                                                                       |

### User Provisioning Rule

| Field                                    | Description                                                                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Available User Provisioning Rules</b> |                                                                                                                                                                               |
| <b>Name</b>                              | The name of the user provisioning rule.                                                                                                                                       |
| +                                        | Assigns the user provisioning rule to the level 1 hierarchy or site.<br><br>The system moves the user provisioning rule to the Selected User Provisioning Rules section.      |
| <b>Selected User Provisioning Rules</b>  |                                                                                                                                                                               |
| <b>Name</b>                              | The name of the user provisioning rule that you selected from the Available User Provisioning Rules section.                                                                  |
| X                                        | Unassigns the user provisioning rule from the level 1 hierarchy or site.<br><br>The system moves the user provisioning rule to the Available User Provisioning Rules section. |

### Level 2 Details or Department Details

The system displays the section when you select a level 1 hierarchy or site, and click **Add**.

| Name               | Description                                                 |
|--------------------|-------------------------------------------------------------|
| <b>Name</b>        | The name of the level 2 hierarchy or department.            |
| <b>Description</b> | A brief description of the level 2 hierarchy or department. |

### Level 3 Details or Team Details

The system displays the section when you select a level 2 hierarchy or department, and click **Add**.

| Name        | Description                                |
|-------------|--------------------------------------------|
| <b>Name</b> | The name of the level 3 hierarchy or team. |

*Table continues...*



| Name        | Description                                           |
|-------------|-------------------------------------------------------|
| Description | A brief description of the level 3 hierarchy or team. |

# Chapter 22: Shutting down System Manager

---

## Overview

System Manager executes several scheduled processes in the background. When System Manager shuts down, the system must stop the processes that System Manager runs in the background. This is to ensure that the system is stable and does not contain incomplete data in any data store when System Manager starts the next time. The system must also ensure that the background process that stops does not leave the system in an unstable state.

The shutdown process stops all running jobs and then shuts down System Manager.

 **Note:**

You cannot cancel the process after you select the shutdown process.

To ensure that System Manager shuts down completely, the shutdown feature provides a user interface that displays all scheduled jobs that are running on System Manager and active user sessions. Based on the criticality and priority of scheduled jobs, the administrator can shut down the system immediately or wait for the scheduled jobs to complete.

- If the administrator chooses to shut down the system, the shutdown service performs the following actions:
  - Sends the shutdown notification to active users so that users can commit or rollback the operation. The shutdown framework waits for the specified grace period that the administrator sets for active users to complete the operations.
  - Sends the shutdown signal to the Scheduler of System Manager to interrupt the running jobs. Scheduler service must not start any new scheduled jobs.
  - Blocks access to the System Manager web console during a shutdown. After the grace period, the system disallows new logins. The system stops all existing sessions when the shutdown begins and redirects the sessions to the Login page. The system displays `Shutdown in progress` message on Login page.
  - Logs an audit message indicating that a request for shutdown is made.
  - Makes an entry in a file about the shutdown request. The system uses the shutdown request information to display the shutdown history.
  - Shuts down all applicable services such as JBoss, Postgres, and CND.

- If any of the steps fail, the system logs a message and performs the next step.
- Administrator can shut down System Manager from the command line interface or System Manager web console.

---

## Shutting down System Manager from the web console

### About this task

When you start the shutdown process, you cannot access the System Manager web console.

### Before you begin

Log on to the System Manager web console of the active server.

### Procedure

1. On the System Manager web console, click **Services > Shutdown > Shutdown System Manager**.
2. In the Running and Pending Scheduled Jobs section, view the running and pending scheduled jobs.
3. In the Active User Sessions section, view the active user sessions.
4. On the System Manager web console, click **Services > Shutdown > Shutdown History**.
5. In Initiate Shutdown, click **Shutdown System Manager**.

System Manager displays the Shutdown System Manager dialog box with the following message.

The system initiates System Manager shut down after the grace period of 10 minutes, and stops all running jobs. Once you click Yes, you cannot abort this operation.

The system notifies all the users who logged in before System Manager shuts down is initiated.

Are you sure you want to shutdown System Manager?

6. To start the shutdown process, click **Yes**.

### Related links

[Edit Profile:GracefulShutdown field descriptions](#) on page 880

[View Profile:GracefulShutdown field descriptions](#) on page 880

---

## Rebooting System Manager virtual machine from the web console

### About this task

When you start the reboot process, you cannot access the System Manager web console.

### Before you begin

Log on to the System Manager web console of the active server.

### Procedure

1. On the System Manager web console, click **Services > Shutdown > Shutdown System Manager**.
2. In the Running and Pending Scheduled Jobs section, view the running and pending scheduled jobs.
3. In the Active User Sessions section, view the active user sessions.
4. In Initiate Reboot, click **Reboot System Manager**.

System Manager displays the Reboot System Manager dialog box with the following message.

The system initiates System Manager reboot after the grace period of 10 minutes, and stops all running jobs. Once you click Yes, you cannot abort this operation.

The system notifies all the users who logged in before System Manager reboot is initiated.

Are you sure you want to Reboot System Manager?

5. To start the reboot process, click **Yes**.

---

## Viewing the shutdown history from the System Manager web console

### Procedure

1. On the System Manager web console, click **Services > Shutdown > Shutdown History**.
2. On the Shutdown History page, you can view the shutdown history of the last shutdown actions.

The Shutdown History page displays the date, time, and status of the shutdown action.

## Shutdown System Manager field descriptions

### Initiate Shutdown

| Button                  | Description                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------|
| Shutdown System Manager | Displays the Shutdown System Manager dialog box to select an option to start the shutdown process. |

### Initiate Reboot

| Button                | Description                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------|
| Reboot System Manager | Displays the Reboot System Manager dialog box to select an option to start the reboot process. |

### Running and Pending Scheduled Jobs

| Name         | Description                                      |
|--------------|--------------------------------------------------|
| Job Name     | The job name as displayed on the Scheduler page. |
| Job Type     | The job type as displayed on the Scheduler page. |
| Job Status   | The status of the job.                           |
| Scheduled By | The name of the user who created the job         |
| Start Time   | The date and time the job is scheduled to start. |

### Active User Sessions

| Name                      | Description                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| User Name                 | The user name who is currently active.                                                                                          |
| Session Duration          | The session duration since when the user is active.                                                                             |
| Is Current Session Status | The status of the current session. The status can be: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> |

# Chapter 23: Solution deployment and upgrade

---

## Solution Deployment Manager

---

### Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications. Solution Deployment Manager supports the operations on the customer's Virtualized Environment and the Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

From Release 7.1 and later, Solution Deployment Manager supports migration of Virtualized Environment-based 6.x, 7.0.x, and 7.1.x applications to Release 8.x and later in the customer's Virtualized Environment. For migrating to Release 8.x, you must use Solution Deployment Manager Release 8.x.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager with Solution Deployment Manager runs on:

- Avaya Aura® Virtualized Appliance: Contains a server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 6.5 hypervisor.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.
- Software-Only environment: Avaya Aura® applications are deployed on the customer-owned hardware and the operating system.

With Solution Deployment Manager, you can do the following in Virtualized Environment and Avaya Aura® Virtualized Appliance models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.

**\* Note:**

When an application is configured with Out of Band Management, Solution Deployment Manager does not support upgrade for that application.

For information about upgrading the application, see the application-specific upgrade document on the Avaya Support website.

- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager
  - AVP Utilities
  - Avaya Aura® Appliance Virtualization Platform, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.
- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 8.1.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

---

## Solution Deployment Manager Client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client must be installed on the computer of the technician. The Solution Deployment Manager client provides the functionality to deploy the OVAs or ISOs on an Avaya-provided server, customer-provided Virtualized Environment, or Software-only environment.

A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances, VMware-based Virtualized Environment, and Software-only environment.
- Upgrade System Platform-based System Manager.

- Upgrade VMware-based System Manager from Release 6.x, 7.x, or 8.0.x to Release 8.1 and later.
- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create the Appliance Virtualization Platform Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze® platform.

**\* Note:**

- You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.
- You must always use the latest Solution Deployment Manager client for deployment.
- You must use Solution Deployment Manager Client 7.1 and later to create the kickstart file for initial Appliance Virtualization Platform installation or recovery.

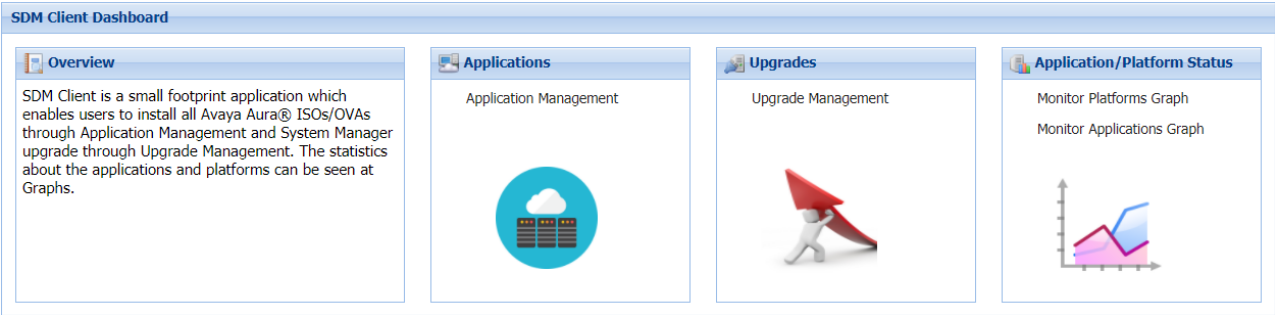


**Figure 1: Solution Deployment Manager Client dashboard**

**Related links**

- [Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client](#) on page 1278
- [Accessing the Solution Deployment Manager client dashboard](#) on page 1283
- [Solution Deployment Manager client capabilities](#) on page 1283

**Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client**

| Centralized Solution Deployment Manager | Solution Deployment Manager Client |
|-----------------------------------------|------------------------------------|
| Manage virtual machine lifecycle.       | Manage virtual machine lifecycle.  |
| Deploy Avaya Aura® applications.        | Deploy Avaya Aura® applications.   |

*Table continues...*



| Centralized Solution Deployment Manager                                                                                                                                                                                                                                                        | Solution Deployment Manager Client                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Deploy hypervisor patches only for Appliance Virtualization Platform.                                                                                                                                                                                                                          | Deploy hypervisor patches only for Appliance Virtualization Platform.           |
| Upgrade Avaya Aura® applications.<br>Release 7.x and later support upgrades from Linux-based or System Platform-based applications to Virtualized Environment or Appliance Virtualization Platform. Release 7.1 and later support Virtualized Environment to Virtualized Environment upgrades. | Upgrade System Platform-based and Virtualized Environment-based System Manager. |
| Install software patches for Avaya Aura® applications excluding System Manager application.                                                                                                                                                                                                    | Install System Manager patches.                                                 |
| Discover Avaya Aura® applications.                                                                                                                                                                                                                                                             | Deploy System Manager.                                                          |
| Analyze Avaya Aura® applications.                                                                                                                                                                                                                                                              | -                                                                               |
| Create and use the software library.                                                                                                                                                                                                                                                           | -                                                                               |

### Related links

[Solution Deployment Manager Client](#) on page 1277

## Installing the Solution Deployment Manager client

### Prerequisites

1. If an earlier version of the Solution Deployment Manager client is running on the computer, remove the older version from **Control Panel > Programs > Programs and Features**.

For information about uninstalling the Solution Deployment Manager client, see “Uninstalling the Solution Deployment Manager client”.

2. Ensure that Windows 7, Windows 8.1 64-bit, Windows 10 64-bit, or Windows 16 64-bit, operating system is installed on the computer.

**+ Tip:**

On **Computer**, right-click properties, and ensure that Windows edition section displays the version of Windows operating system.

3. Ensure that at least 5 GB of disk space is available at the location where you want to install the client. To deploy applications, you must have additional 15 GB of disk space on your system.

**+ Tip:**

Using the Windows file explorer, click **Computer**, and verify that the Hard Disk Drives section displays the available disk space.

4. To avoid port conflict, stop any application server that is running on your computer.

**+ Tip:**

From the system tray, open the application service monitor, select the application server that you want to stop, and click **Stop**.

5. Ensure that the firewall allows the ports that are required to install the Solution Deployment Manager client installation and use the Solution Deployment Manager functionality.

 **Note:**

Ensure that port 8005 or 8009 is available for installing and running Solution Deployment Manager Client. If port 8005 or 8009 is assigned to any other application, you must free up the ports for starting the Avaya SDM service.

For more information, see *Troubleshooting Avaya Aura® System Manager*.

System Manager 8.1.3 Port Matrix lists all the ports and protocols that System Manager uses. You can access the System Manager 8.1.3 Port Matrix document on the Avaya Support website at <http://support.avaya.com/> by using valid credentials.

6. Ensure that ports support Avaya Aura® 8.1.3 supported browsers.
7. Close all applications that are running on your computer.
8. Do not set CATALINA\_HOME as environment variable on the computer where you install the Solution Deployment Manager client.

 **Tip:**

On **Computer**, right-click properties, and perform the following:

- a. In the left navigation pane, click **Advanced system settings**.
  - b. On the System Properties dialog box, click the **Advanced** tab, and click **Environment Variables**.
  - c. Verify the system variables.
9. Ensure that the computer on which the Solution Deployment Manager client is running is connected to the network.

Operations that you perform might fail if the computer is not connected to the network.

## Related links

[Solution Deployment Manager Client](#) on page 1277

## Installing the Solution Deployment Manager client on your computer

### About this task

In Avaya Aura® Virtualized Appliance offer, when the centralized Solution Deployment Manager on System Manager is unavailable, use the Solution Deployment Manager client to deploy the Avaya Aura® applications.

You can use the Solution Deployment Manager client to install software patches of only System Manager and hypervisor patches of Appliance Virtualization Platform.

Use the Solution Deployment Manager client to deploy, upgrade, and update System Manager.

From Avaya Aura® Appliance Virtualization Platform Release 7.0, Solution Deployment Manager is mandatory to upgrade or deploy the Avaya Aura® applications.

## Procedure

1. Download the `Avaya_SDMClient_win64_8.1.3.0.1035538_49.zip` file from the Avaya Support website at <http://support.avaya.com> or from the Avaya PLDS website, at <https://plds.avaya.com/>.
2. On the Avaya Support website, click **Support by Products > Downloads**, and type the product name as **System Manager**, and Release as **8.1.x**.
3. Click the **Avaya Aura® System Manager Release 8.1.x SDM Client Downloads, 8.1.x** link. Save the zip file, and extract to a location on your computer by using the WinZip application.

You can also copy the zip file to your software library directory, for example, `c:/tmp/Aura`.

4. Right click on the executable, and select **Run as administrator** to run the `Avaya_SDMClient_win64_8.1.3.0.1035538_49.exe` file.

The system displays the Avaya Solution Deployment Manager screen.

5. On the Welcome page, click **Next**.
6. On the License Agreement page, read the License Agreement, and if you agree to its terms, click **I accept the terms of the license agreement** and click **Next**.
7. On the Install Location page, perform one of the following:
  - To install the Solution Deployment Manager client in the system-defined folder, leave the default settings, and click **Next**.

If the `C:\Program Files\Avaya\AvayaSDMClient` directory is not empty, the installer displays the following message: To install the SDM client, select an empty directory or manually delete the files from the installation directory.

If the file is locked and you are unable to delete it, reboot the machine, and then delete the file.

- To specify a different location for installing the Solution Deployment Manager client, click **Choose**, and browse to an empty folder. Click **Next**.

To restore the path of the default directory, click **Restore Default Folder**.

The default installation directory of the Solution Deployment Manager client is `C:\Program Files\Avaya\AvayaSDMClient`.

8. On the Pre-Installation Summary page, review the information, and click **Next**.
9. On the User Input page, perform the following:
  - a. To start the Solution Deployment Manager client at the start of the system, select the **Automatically start SDM service at startup** check box.
  - b. To change the default software library directory on windows, in Select Location of Software Library Directory, click **Choose** and select a directory.

The default software library of the Solution Deployment Manager client is  
C:\Program Files\Avaya\AvayaSDMClient\Default\_Artifacts.

You can save the artifacts in the specified directory.

- c. In **Data Port No**, select the appropriate data port.

The default data port is 1527. The data port range is from 1527 through 1627.

- d. In **Application Port No**, select the appropriate application port.

The default application port is 443. If this port is already in use by any of your application on your system, then the system does not allow you to continue the installation. You must assign a different port number from the defined range. The application port range is from 443 through 543.

 **Note:**

After installing the Solution Deployment Manager client in the defined range of ports, you cannot change the port after the installation.

- e. (Optional) Click **Reset All to Default** to reset all values to default.

10. Click **Next**.

11. On the Summary and Validation page, verify the product information and the system requirements.

The system performs the feasibility checks, such as disk space and memory. If the requirements are not met, the user must make the required disk space, memory, and the ports available to start the installation process again.

12. Click **Install**.

13. On the Install Complete page, click **Done** to complete the installation of Solution Deployment Manager Client.

Once the installation is complete, the installer automatically opens the Solution Deployment Manager client in the default web browser and creates a shortcut on the desktop.

14. To start the client, click the Solution Deployment Manager client icon, .

## Next steps

- Configure the laptop to get connected to the services port if you are using the services port to install.
- Connect the Solution Deployment Manager client to Appliance Virtualization Platform through the customer network or services port.

For information about “Methods to connect the Solution Deployment Manager client to Appliance Virtualization Platform”, see *Using the Solution Deployment Manager client*.

## Related links

[Solution Deployment Manager Client](#) on page 1277

## Accessing the Solution Deployment Manager client dashboard

### About this task

#### \* Note:

If you perform deploy, upgrade, and update operations from the Solution Deployment Manager client, ignore the steps that instruct you to access System Manager Solution Deployment Manager and the related navigation links.

### Procedure

To start the Solution Deployment Manager client, do one of the following:

- On your computer, click **Start > All Programs > Avaya > Avaya SDM Client**.
- On your desktop, click .

### Related links

[Solution Deployment Manager Client](#) on page 1277

## Solution Deployment Manager client capabilities

The Solution Deployment Manager client provides the following capabilities and functionality:

- Runs on the following operating systems:
  - Windows 7, 64-bit Professional or Enterprise
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
  - Windows Server 2016, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deployment of System Manager. The Solution Deployment Manager client is the only option to deploy System Manager.
- Supports the Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of Avaya Aura® applications.
- Defines the physical location, Avaya Aura® Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

#### \* Note:

For the Avaya Aura® Messaging element, trust re-establishment is not required.

- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.

**\* Note:**

- System Manager must be on the same or higher release than the application you are upgrading to. For example, you must upgrade System Manager to 7.1.3.2 before you upgrade Communication Manager to 7.1.3.2.

All the applications that are supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for the version of applications that are supported by System Manager, see Avaya Aura® Release Notes on the Avaya Support website.

- Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 7.1.3 OVA, Solution Deployment Manager Client version must be on Release 7.1.3, 7.1.3.1, 7.1.3.2, or 8.0. Solution Deployment Manager Client cannot be on Release 7.1.
- Configures application and networking parameters required for application deployments.
- Supports selecting the application OVA file from a local path or an HTTPS URL. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

**\* Note:**

To install the patch on System Manager, Solution Deployment Manager Client must be on the same or higher release as the patch. For example, if you are deploying the patch for System Manager Release 7.1.1, you must use Solution Deployment Manager Client Release 7.1.1 or higher.

However, to install the patch on System Manager Release 7.0.x, Solution Deployment Manager Client must be on Release 7.0.x.

Avaya Aura® applications use centralized Solution Deployment Manager from System Manager to install software patches, service packs, and feature packs. For the applications that cannot be patched from centralized Solution Deployment Manager, use the application Command Line Interface or web console.

For more information about supported releases and patching information, see Avaya Aura® Release Notes on the Avaya Support website.

- Configures Remote Syslog Profile.
- Creates the Appliance Virtualization Platform Kickstart file.

**Related links**

[Solution Deployment Manager Client](#) on page 1277

---

## Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following applications:

- AVP Utilities 8.1.3
- System Manager 8.1.3
- Session Manager 8.1.3
- Branch Session Manager 8.1.3
- Communication Manager 8.1.3
- Application Enablement Services 8.1.3
- WebLM 8.1.3
- Communication Manager Messaging 7.0

For information about other Avaya product compatibility information, go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

With Solution Deployment Manager, you can migrate, upgrade, and update the following applications:

- Hardware-based Session Manager 6.x
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

 **Note:**

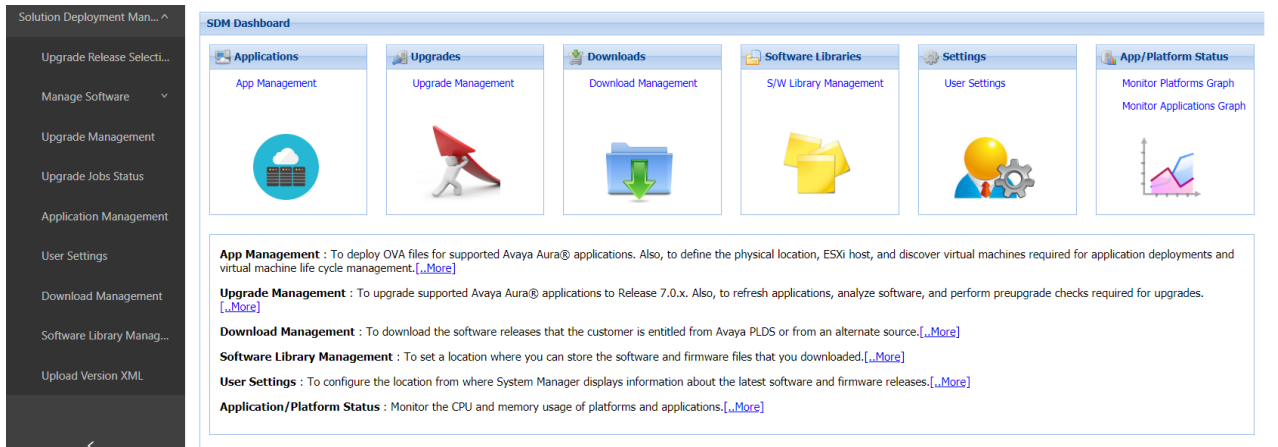
You must manually migrate the Services virtual machine that is part of the template.



The centralized deployment and upgrade process provides better support to customers who want to upgrade their systems to Avaya Aura® Release 8.1.3. The process reduces the upgrade time and error rate.

### Solution Deployment Manager dashboard

You can gain access to the Solution Deployment Manager dashboard from the System Manager web console or by installing the Solution Deployment Manager client.



### Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting:** To select **Release 7.x Onwards** or **6.3.8** as the target upgrade. Release 8.1.3 is the default upgrade target.
- **Manage Software:** To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application Management:** To deploy OVA files for the supported Avaya Aura® application.
  - Configure Remote Syslog Profile.
  - Generate the Appliance Virtualization Platform Kickstart file.
- **Upgrade Management:** To upgrade Avaya Aura® applications to Release 8.1.3.
- **User Settings:** To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management:** To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management:** To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML:** To save the `version.xml` file to System Manager. You require the application-specific `version.xml` file to perform upgrades.



---

# Solution Deployment Manager configuration settings

---

## User settings

You require the PLDS connection to gain access to Avaya from where you can obtain all software and firmware files that are required for upgrade, migration, and updates. Ensure that you add the required ports and websites to the customer firewall. For example, you require access to the ftp.avaya.com website to get the `versions.xml` and http to grant access to plds.avaya.com. If the customer decides not to open PLDS in the organization firewall, an alternate source must be set to access the software. For example, if the customer wants to test the latest versions of software before using the software for production. By using the alternate source, the customers can get the software that is recommended by the analyze operation.

---

## Establishing PLDS connection to Avaya

### About this task

Use the procedure to configure the location from where System Manager displays information about the latest software and firmware releases during Analyze operation. The entitlements depend on the credentials that you provide on the **User Settings** page.

### Before you begin

- Obtain a company ID to configure PLDS.
- Add the required ports and websites to a firewall of customer.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > User Settings**.
2. On the User Settings page, click **Edit**.
3. Select the **Use Avaya Support Site** check box, and provide the SSO user name and SSO password for PLDS, and the company ID.
4. Configure the PLDS settings and proxy settings for the software download.
5. If your network configuration requires a proxy, select the **Use Proxy** check box, and provide the details.
6. Click **Commit**.

### Related links

[Obtaining a company ID](#) on page 1288

[User Settings field descriptions](#) on page 1291

## Obtaining a company ID

### Before you begin

Ensure that you have access and user credentials to log in to the PLDS website at <https://plds.avaya.com>.

### Procedure

1. On the web browser, type the PLDS URL, `https://plds.avaya.com`.
2. In the **Email address** field, enter the user name, and in the **Password** field, enter the password.
3. Click **Submit**.
4. After successful log in, on the Home page, click **Administration > My Company**.

The system displays the company ID followed by a company name.

---

## Establishing the connection to an alternate source

### About this task

If you decide to close the PLDS website in the customer firewall, an alternate source must be configured to get the software. For example, if you want to test the latest versions of software before using the software for production.

### Before you begin

To use an alternate source:

1. Set up the HTTP server for alternate-source and create a directory with a valid name, such as `alternate-source` in the `http://<ip-address>OR<FQDN>/<alternate-source>` location.

Ensure that the URL `http://<ip-address>OR<FQDN>/<alternate-source>` is accessible through the web browser.

2. From PLDS website, download the `smgr-versionsxmls.zip` file.

For more information, see “Downloading the `smgr-versionsxmls.zip` file from PLDS”.

3. Copy the following xml files to the `alternate-source` directory:

- `versions.xml`
- `versions_aams.xml`
- `versions_aes.xml`
- `versions_avutilities.xml`
- `versions_bsm.xml`
- `versions_cmm.xml`
- `versions_compatibility.xml`

- versions\_edp.xml
- versions\_msg.xml
- versions\_others.xml
- versions\_sbce.xml
- versions\_sp.xml
- versions\_systemplatform.xml
- versions\_avp.xml
- versions\_us.xml
- versions\_weblm.xml

4. From PLDS, download the software on your computer, and copy to the `http://<ip-address>/FQDN/<alternate-source>/` location for the following:

- For Communication Manager upgrades: Communication Manager, Communication Manager Messaging, Branch Session Manager, Session Manager, Appliance Virtualization Platform, Utility Services, TN boards, and Media Gateways or media modules based on your entitlements.
- For IP Office upgrades: IP Office Manager Admin Lite, VM Pro Client, IP Office, Unified Communications Module (UCM), and IP Office Application Server binary files.

 **Note:**

You cannot use My Computer on the File Download Manager page to upload IP Office Manager Admin Lite, VMPro Client, UCM, and IP Office Application Server binary files.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **User Settings**.
3. On the User Settings page, click **Edit**.
4. Clear the **Use Avaya Support Site** check box.
5. In **Alternate Source**, type the server path for an alternate source, that is mentioned in the prerequisites.

 **Note:**

The IP address for the alternate source and the software library can be the same. However, ensure that locations for the alternate source URL and software library server path in software library configuration are different. To configure an alternate source and software library on the same server with the artifacts, allocate at least 20 GB disk space each for alternate source and software library.

The size depends on the number of artifacts that you want to save in the alternate source and the number of artifacts that you want to download in the software library during the upgrade.

6. Click **Commit**.

7. Download the specified xml files on your computer.

For help to download contact the Avaya support team.

8. Upload the xml files to the HTTP server.

9. Download the required firmware files from PLDS.

To download the firmware files, contact the Avaya support team.

10. Upload the firmware files to the http server.

Ensure that you update the firmware files and the xml files in the http server from `ftp.avaya.com`.

#### Related links

[Downloading the smgr-versionsxmls.zip file from PLDS](#) on page 1290

## Downloading the smgr-versionsxmls.zip file from PLDS

### Before you begin

Log on to PLDS.

### Procedure

1. On the PLDS web console, click **Assets > View Downloads**.

2. Click **Search by Download**.

3. In the **Download pub ID**, enter `SMGRSUM0001`.

4. Click **Search Downloads**.

5. In the search results, click **Download**.

The system prompts you to save the ZIP file on your local computer.

6. Extract the ZIP file on your local computer.

#### Related links

[Establishing the connection to an alternate source](#) on page 1288

## User Settings field descriptions

### Source configuration

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use Avaya support site</b> | <p>The option to find the information and download the software releases from the Avaya Support website.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>To download the firmware and analyze the software on System Manager, you must gain access to <code>plds.avaya.com</code>, <code>pldsxml.avaya.com</code>, and <code>downloads.avaya.com</code>.</li> <li>Select the <b>Use Avaya Support Site</b> check box, to use <b>Avaya Support Site</b>. Enter the SSO user name, SSO password, and Company ID details. The SSO authentication is required to get entitlements for <b>Analyze</b> and artifacts for download.</li> <li>If you select the check box, the <b>Alternate Source</b> is unavailable.</li> </ul>                                                                                                           |
| <b>Alternate Source</b>       | <p>The website location from where you can get the latest software. The alternate source is an HTTP URL and an alternate to the Avaya Support website. You must set the alternate source. For more information, see <i>Setting up an alternate source</i>.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>The XML files compare the available software version and the latest available version in PLDS.</li> <li>Clear the <b>Use Avaya Support Site</b> check box, to use alternate source repository. You must enter a http URL, for example: <code>http://148.147.216.220/SUMDATA/</code>.</li> <li>The IP address of the alternate source can be the same as the IP address of the software library. However, ensure that the URL location and the server path for software library configuration are different.</li> </ul> |

### PLDS configuration

| Name                        | Description                                      |
|-----------------------------|--------------------------------------------------|
| <b>SSO User Name</b>        | The user name used as a single sign on for PLDS. |
| <b>SSO Password</b>         | The single sign on password for PLDS.            |
| <b>Confirm SSO Password</b> | The SSO password that you retype in this field.  |

*Table continues...*

| Name              | Description                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Company ID</b> | <p>The company ID for PLDS. For more information, see Obtaining a company ID.</p> <p> <b>Note:</b></p> <p>After upgrading System Manager, if the system does not auto populate the <b>Company ID</b> field, then you must manually edit the field with appropriate value after the upgrade.</p> |

## Proxy settings

You require proxy settings to use the Avaya PLDS and the Avaya Support site. If your network configuration requires a proxy, enter the details in the **Proxy Settings** section.

| Name                    | Description                                                                     |
|-------------------------|---------------------------------------------------------------------------------|
| <b>Use Proxy</b>        | The option to use the proxy server for PLDS.                                    |
| <b>Host</b>             | The host name of the proxy.                                                     |
| <b>Port</b>             | The port of the proxy.                                                          |
| <b>Password</b>         | The password of the proxy server for the Avaya Support website.                 |
| <b>Confirm Password</b> | The password of the proxy server that you retype for the Avaya Support website. |

| Button        | Description                                                      |
|---------------|------------------------------------------------------------------|
| <b>Edit</b>   | To display the edit page where you can change the user settings. |
| <b>Commit</b> | To save the user settings that you enter.                        |
| <b>Reset</b>  | To reset the page and clear the values that you enter.           |
| <b>Cancel</b> | To cancel your action and return to the previous page.           |

---

# Software library management

---

## Software library

Using software library, you can store the software and firmware files that you download. After you download a firmware file in the Software Library, you can use the downloaded file across multiple devices.

With software library, you can also create, modify, view, and delete the firmware files.

For upgrading the firmware files, use an external server that functions as a remote software library. To upload the firmware files from System Manager, you must configure an FTP, SCP, or SFTP protocol for the external server.

**\* Note:**

- A local, non-editable software library, SMGR\_DEFAULT\_LOCAL, resides within System Manager post installation. You require only remote software library for upgrading TN boards and IP Office. For upgrading other elements, you can use a local or remote library.
- The system downloads the TN boards firmware files at home directory of the SCP user configured on the **SCP Configuration** tab of Remote SCP S/W Library irrespective of the path configured in the **Server Path** field on the **Library Server Details (L)** tab of the Add Software Library page.

### Related links

[Editing a software library](#) on page 1304

[Viewing a software library](#) on page 1304

[Deleting a file from the software library](#) on page 1309

[System requirements for the external server](#) on page 1310

[Software library field descriptions](#) on page 1305

[Software Library Files field descriptions](#) on page 1309

---

## Enabling and disabling FTP on System Manager

### About this task

You must enable FTP on System Manager only to use System Manager as a local software library for upgrading Media Gateway and Media Modules.

**\* Note:**

When the upgrade is complete, disable FTP only to re-enable when you need.

### Before you begin

Start an SSH session.

### Procedure

1. Log on to the System Manager web console with administrator privilege credentials.
2. To enable the FTP server, do the following:
  - a. At the prompt, type `sh/opt/vsp/SDM_FTP_Patch/Setup.sh`.
  - b. Type the sdmuser password and press `Enter`.

You can now use the FTP library to save the software or firmware.

3. To disable the FTP server, type `sh/opt/vsp/SDM_FTP_Patch/Setup.sh stop`.

---

## Configuring System Manager as local software library

### About this task

Use the procedure to configure System Manager as local FTP server to save the software for Media Modules and Media Gateways for upgrades. However, you can also use the remote FTP server.

#### **Note:**

Use only remote FTP server as software library to save the TN Board firmware. You cannot use System Manager as software library.

### Before you begin

Enable FTP on System Manager.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Select SMGR\_DEFAULT\_LOCAL and click **Edit**.

The system displays the Edit Software Library page.

4. On the Library Server Details (L) tab, in **Default Protocol**, click **FTP**.
5. Click the FTP Configuration (F) tab, and select the **Enable FTP** check box.
6. In **User Name**, type `sdmuser`.

The system preconfigures the ftpuser name when you run the script as described in “Enabling and disabling FTP on System Manager”. You cannot change the user name.

7. In **Password** and **Confirm Password** fields, type the same password that you configured while running the script.
8. Click **Commit**.
9. In the left navigation pane, click **Download Management** and download the required Media Gateway/Media Module firmware in the SMGR\_DEFAULT\_LOCAL software library.

---

## Configuring external server as a remote software library for upgrades

### Protocol requirements to configure a remote server

To configure an external server as a remote software library, you must configure HTTP, FTP, SCP, or SFTP protocol on the external server. For the external server that you select, you must install separate executable files as listed in the following table:



| External server                    | File for deployment                       |
|------------------------------------|-------------------------------------------|
| Apache HTTP server                 | httpd-2.0.64-win32-x86-openssl-0.9.8o.msi |
| FileZilla FTP server               | FileZilla_Server-0_9_43.exe               |
| Linux <sup>®</sup> SCP/SFTP server | SftpServerInstaller.msi                   |

**\* Note:**

Do not use the SolarWinds SCP/SFTP server to configure the software library for upgrades. System Manager might become nonfunctional. Instead, use the Linux<sup>®</sup> server.

For every release of the Avaya Aura<sup>®</sup> application that you want to upgrade, you require a combination of protocols listed in the table. The information applies only for the Windows environment.

**\* Note:**

If you use multiple protocols, use the same user name or same directory for all protocols.

| Device for upgrade                       | Required protocols                                                                                                                                                                                                               |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Avaya Aura <sup>®</sup> 6.x applications | <ul style="list-style-type: none"> <li>• HTTP/HTTPS</li> <li>• FTP/SCP</li> </ul>                                                                                                                                                |
| Communication Manager 5.2.1 release      | <ul style="list-style-type: none"> <li>• FTP</li> </ul> <p><b>* Note:</b></p> <p>For upgrading the Communication Manager 5.2.1 release, use the FTP protocol.</p> <ul style="list-style-type: none"> <li>• HTTP/HTTPS</li> </ul> |

## Related links

[Installing and configuring an HTTP server as a remote server](#) on page 1295

[Installing and configuring an FTP server as a remote server](#) on page 1296

[Installing and configuring an SCP or SFTP server as a remote server](#) on page 1299

## Installing and configuring an HTTP server as a remote server

### Procedure

1. Run `httpd-2.0.64-win32-x86-openssl-0.9.8o.msi` as an administrator.
2. Type the domain name, server name and email ID.
3. Complete the installation.
4. Start the application server.
5. In the `C:\Program Files(x86)\Apache Group\Apache2\htdocs\` location, create a folder named `downloads`.

For example, `C:\Program Files(x86)\Apache Group\Apache2\htdocs\downloads\`

6. Provide the `downloads` folder with full privileges.

7. To verify the privileges, do the following:
  - a. Add a file to the `downloads` folder.
  - b. Open the file from the browser.

## Result

On the System Manager web console, on the Software Library Configuration page, the Library Server Details tab displays the following details:

Library Server Details (L) \* SCP Configuration (S) SFTP Configuration (T) FTP Configuration (F) HTTP/HTTPS Configuration (H)

Remote Library ☒

Local Survivable Processor (LSP) ☐

\* Name

\* IP Address

Description

\* Server Path

Default Library ☐

\* Default Protocol  (Enter the values for the mandatory fields in the protocol configuration tab you selected.)

The HTTP/HTTPS Configuration tab displays the following http/https configuration details:

Library Server Details (L) \* SCP Configuration (S) SFTP Configuration (T) FTP Configuration (F) HTTP/HTTPS Configuration (H)

Enable HTTP/HTTPS ☒

\* URL

User Name

Password

Confirm Password

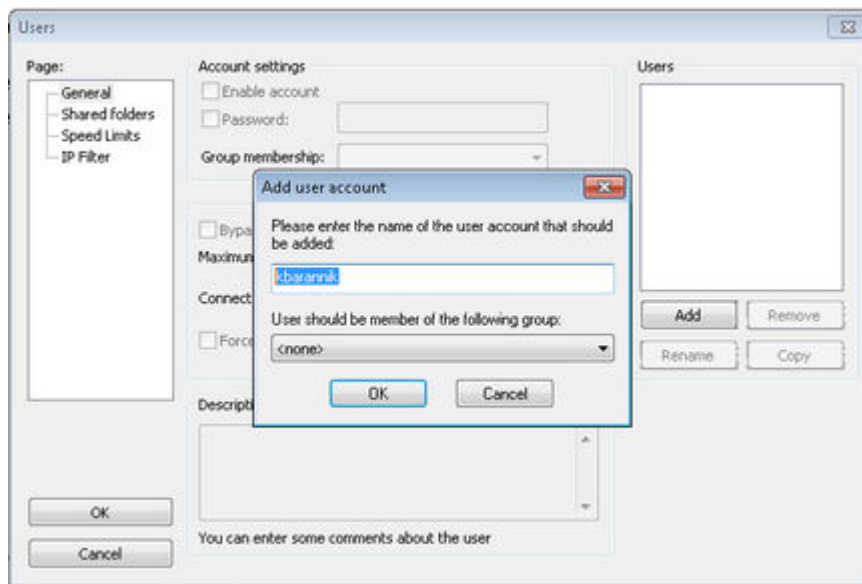
## Related links

[Protocol requirements to configure a remote server](#) on page 1294

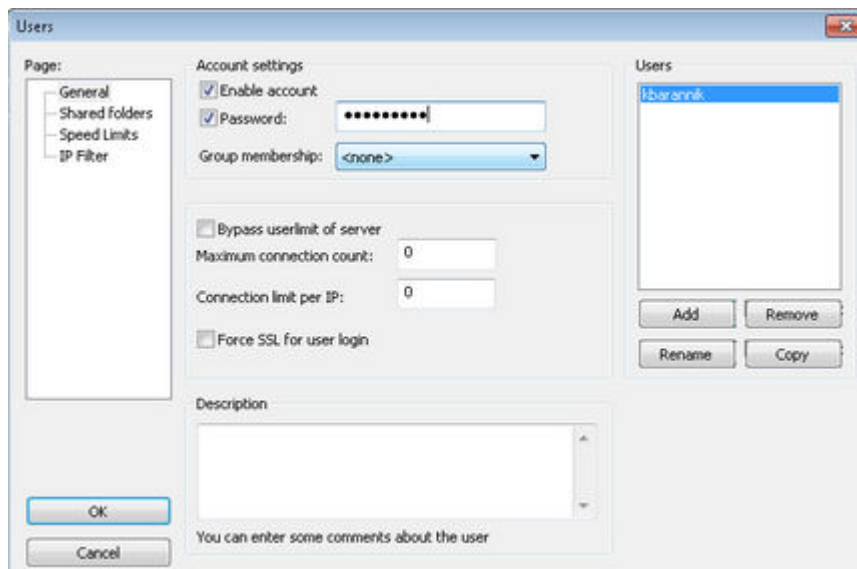
## Installing and configuring an FTP server as a remote server Procedure

1. Run `FileZilla_Server-0_9_43.exe` as an administrator.  
Wait until the installation is complete.
2. Open the FileZilla server interface.
3. On the **Edit** menu, click **Users**.
4. In the Users dialog box, in the left navigation pane, click **General**.

5. In the **Users** section, click **Add**.



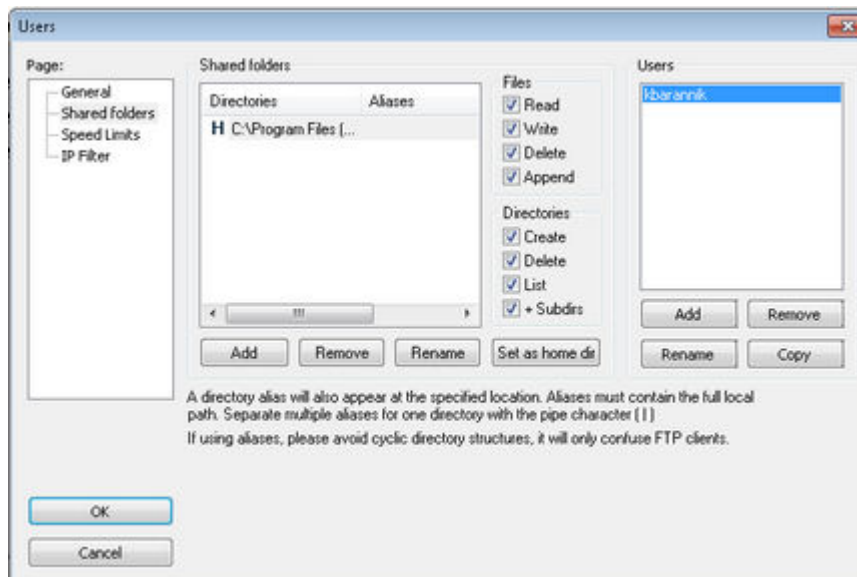
6. In the Add user account dialog box, type a user name and click **OK**.  
 7. Select the **Password** check box.  
 8. Type a password and click **OK**.



The system prompts you to provide a folder.

9. In the left pane, click **Shared folders**.  
 10. In the **Shared folders** section, click **Add** and provide the folder location till the `downloads` folder.  
 11. Click **OK**.

12. To provide the privileges, in the **Files** section, select the check boxes, such as **Read**, **Write**, and **Delete**.



13. To set the `downloads` folder as the home directory, do the following:
  - a. Click **Set as home dir** and navigate to the `C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\` folder.
  - b. Click **OK**.

**! Important:**

Ensure that you select a logical file name option. By default, the system selects `/C/`.



14. To verify the privileges, using the **FTP** client, navigate to the `downloads` folder and open a file.

**Result**

On the System Manager web console, on the **Software Library Configuration** page, the FTP Configuration tab displays the following FTP configuration details:

The screenshot shows the 'FTP Configuration (F)' tab of the SolarWinds SFTP/SCP Server configuration window. It includes the following fields and options:

- Enable FTP**: A checked checkbox.
- \* User Name**: A text field containing 'kbarannik'.
- \* Password**: A password field with masked characters (dots).
- \* Confirm Password**: A second password field with masked characters (dots).

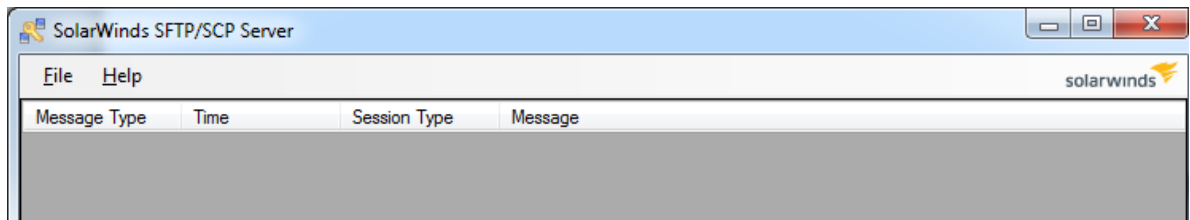
At the top of the window, there are tabs for 'Library Server Details (L)', 'SCP Configuration (S)', 'SFTP Configuration (T)', 'FTP Configuration (F)', and 'HTTP/HTTPS Configuration (H)'.

## Related links

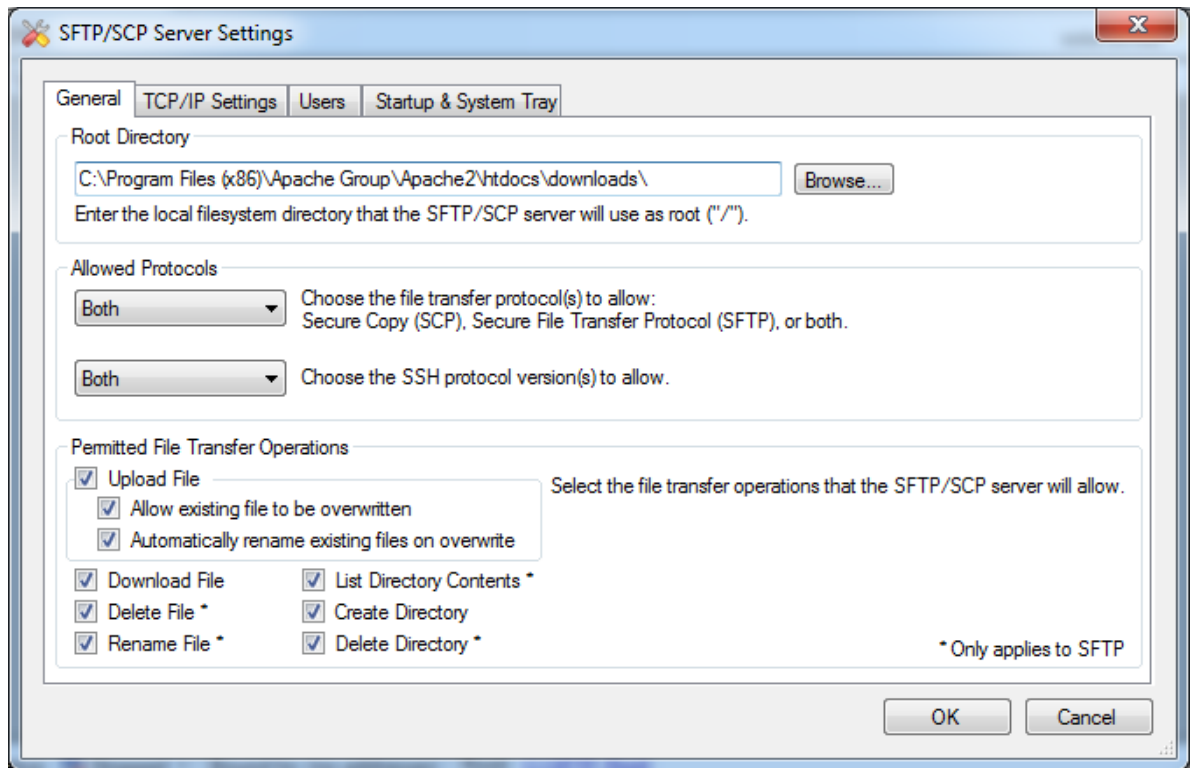
[Protocol requirements to configure a remote server](#) on page 1294

## Installing and configuring an SCP or SFTP server as a remote server Procedure

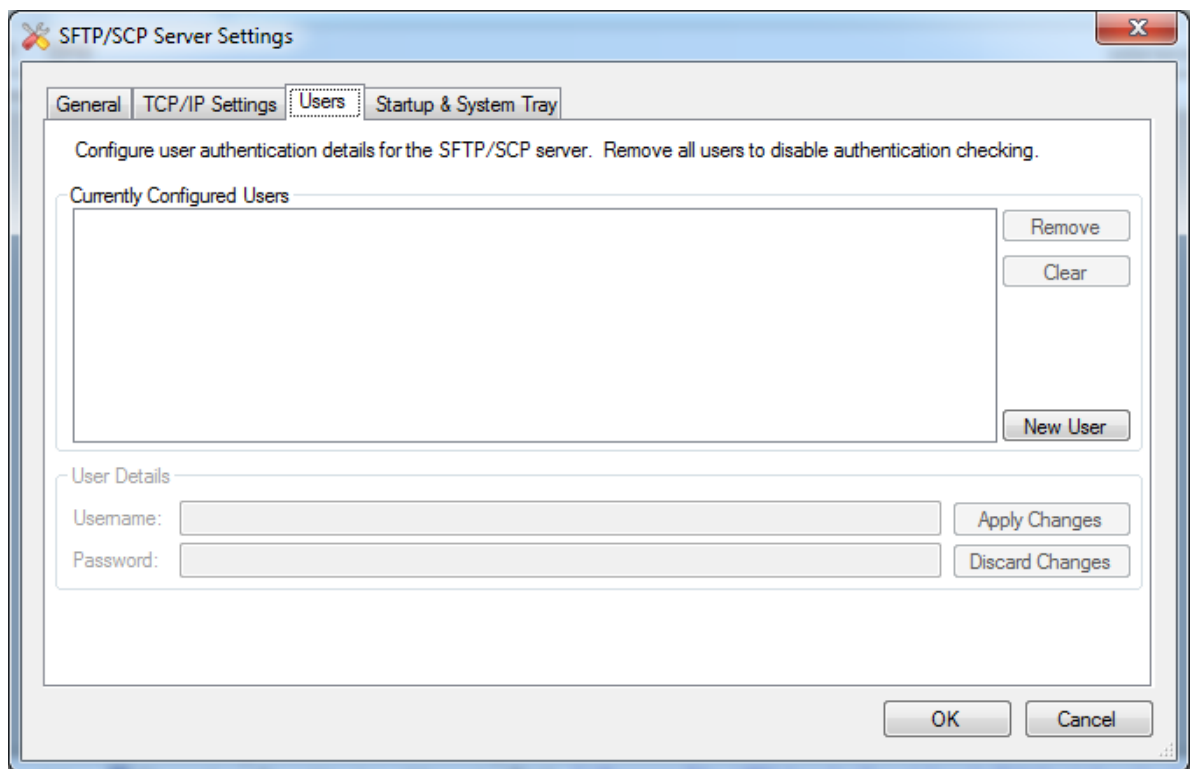
1. Run `SftpServerInstaller.msi` as administrator.  
Wait until the installation is complete.
2. Open the **SolarWinds SFTP & SCP Server** server interface.



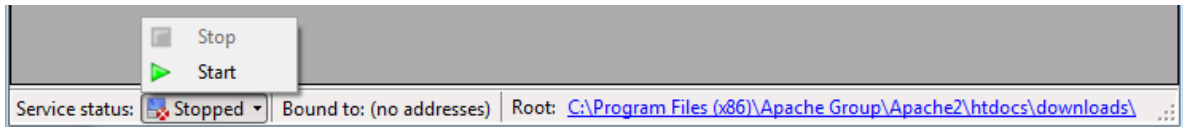
3. On the **File** menu, click **Configure**.
4. Navigate to `C:\Program Files (x86)\Apache Group\Apache2\htdocs\downloads\`.
5. Set the required parameters and click **OK**.



6. Click the Users tab.



7. Click **New User**.
8. Enter the user name and the password.
9. Click **Apply Changes**.
10. Start the server.



11. To verify the privileges, using the SCP or the SFTP client, navigate to the `downloads` folder and open a file.

## Result

On the Software Library Configuration page of System Manager, the **SCP Configuration** tab displays the following:

 A screenshot of the 'SCP Configuration' tab in a web interface. It shows a form with the following fields: 'Enable SCP' (checked), 'User Name' (kbarannik), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). The tab is part of a larger configuration page with other tabs like 'Library Server Details', 'SFTP Configuration', 'FTP Configuration', and 'HTTP/HTTPS Configuration'.

## Related links

[Protocol requirements to configure a remote server](#) on page 1294

## Installing and configuring an HTTP server as a remote server on a Linux server

### About this task

Use this procedure for System Platform-based Element upgrade. The HTTP protocol is used to pull the downloaded artifacts files during element upgrade.

### Before you begin

- Install the FTP/SCP Software on the Linux server.
- Install the HTTP server software on the Linux server.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. On the Software Library page, click **New**.  
The system displays the Add Software Library page.
4. On the **Library Server Details** tab, perform the following:
  - a. In **Name**, type the Linux server name.

- b. In **IP Address**, type the IP address of the Linux server.
- c. In **Server Path**, type the path where artifacts will be downloaded on Linux based FTP/SCP Software Library by using the FTP/SCP protocol.
- d. In **Default Protocol**, click **FTP**.

The screenshot shows the 'Library Server Details' window with the 'FTP Configuration (F)' tab selected. The 'Remote Library' checkbox is checked. The 'Local Survivable Processor (LSP)' checkbox is unchecked. The 'Name' field is 'Linux\_SwLib'. The 'IP Address' field is '148.147.162.215'. The 'Description' field is empty. The 'Server Path' field is '/home/ftpuser/'. The 'Default Library' checkbox is checked. The 'Default Protocol' dropdown is set to 'FTP'. A note at the bottom says '(Enter the values for the mandatory fields in the protocol configuration tab you selected.)'. At the bottom right are 'Commit', 'Reset', and 'Cancel' buttons.

5. On the **FTP Configuration** tab, perform the following:
  - a. Select the **Enable FTP** check box.
  - b. In **User Name**, type the FTP server user name.
  - c. In **Password**, type the FTP server password.
  - d. In **Confirm Password**, retype the FTP server password.

The screenshot shows the 'Library Server Details' window with the 'FTP Configuration (F)' tab selected. The 'Enable FTP' checkbox is checked. The 'User Name' field is 'ftpuser'. The 'Password' field is masked with dots. The 'Confirm Password' field is also masked with dots. At the bottom right are 'Commit', 'Reset', and 'Cancel' buttons.

6. On the **HTTP/HTTPS Configuration** tab, perform the following:
  - a. Select the **Enable HTTP/HTTPS** check box.
  - b. In **URL**, type the HTTP/HTTPS URL.

The example URL is: `http://<LinuxServerIPAddress>/`.

The screenshot shows the 'Library Server Details' window with the 'HTTP/HTTPS Configuration (H)' tab selected. The 'Enable HTTP/HTTPS' checkbox is checked. The 'URL' field is 'http://148.147.162.215/'. The 'User Name' field is empty. The 'Password' field is empty. The 'Confirm Password' field is empty. At the bottom right are 'Commit', 'Reset', and 'Cancel' buttons.

7. Click **Commit**.
8. To complete the configuration add the `/home/ftpuser/ "/home/ftpuser/"` alias in the HTTP server configuration `httpd.conf` file.
  - a. Change the DocumentRoot to `/home/<FTP/SCP_username_dir>` in the `/etc/httpd/conf/httpd.conf` file.

For example:



```
sed -i 's~/var/www/html~/home/ftpuser~g' httpd.conf
```

```
sed -i 's~/var/www~/home~g' httpd.conf
```

- b. Make apache as primary group for <FTP/SCP\_username\_dir> in the /etc/group folder.

For example:

```
usermod -g 48 ftpuser
```

- c. Change permission of /home/<FTP/SCP\_username\_dir> to 755.

```
chmod 755 -R /home/ftpuser/
```

- d. Add exception in SELinux for httpd or disable SELinux.

If SELinux is already enabled after making above changes, reboot the system.

- e. Add rule in firewalld or stop firewalld.

- f. Add alias in the httpd.conf file as shown below:

```
Alias /home/<FTP/SCP_username_dir> "/home/<FTP/SCP_username_dir>"
```

```
<Directory> "/home/cgi-bin">
 AllowOverride None
 Options None
 Require all granted
</Directory>
```

For example:

```
Alias /home/ftpuser "/home/ftpuser"
```

```
<Directory> "/home/cgi-bin">
 AllowOverride None
 Options None
 Require all granted
</Directory>
```

- g. Restart the httpd service.

## Creating a software library

### Before you begin

For upgrades to Release 6.3.8, create the new EPW file for the Communication Manager to be upgraded, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server. For more information, contact the Avaya support team.

#### **Note:**

You cannot set System Manager as a software library. You must set an external server as a software library.

For more information, see *Protocol requirements for configuring a remote server*.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Software Library Management**.
2. Click **New**.
3. Complete the Add Software Library page.
4. Click **Commit**.
  - To reset the page, click **Clear Configuration**.

---

## Editing a software library

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Select the software library whose details you want to edit.
4. Click **Edit**.
5. Edit the required fields in the Edit Software Library page, and click **Commit**.

---

## Viewing a software library

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Select the software library whose details you want to view.
4. Click **View**.

The system displays the details of the software library you selected on the View Software Library page.

---

## Deleting a software library

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Select the software library you want to delete.
4. Click **Delete**.

5. On the confirmation page, click **Delete**.

## Software library field descriptions

### Library Server Details (L)

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Remote Library</b>                  | <p>An option to select a remote library to:</p> <ul style="list-style-type: none"> <li>• Download files to a remote software library.</li> <li>• Indicate that the local software library is hosted on another server, and not on System Manager.</li> </ul> <p>The system selects the <b>Remote Library</b> option by default.</p>                                                                                                                    |
| <b>Local Survivable Processor(LSP)</b> | <p>An option to select the survivable remote server to add as a software library. The <b>Local Survivable Processor(LSP)</b> option applies only for gateways, and supports FTP and SCP only.</p>                                                                                                                                                                                                                                                      |
| <b>Name</b>                            | The name of the software library.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>IP Address</b>                      | <p>The IP address of the software library.</p> <p>If you select <b>Local Survivable Processor(LSP)</b> , the <b>IP Address</b> field displays the list of survivable remote servers that are added to the System Manager inventory.</p>                                                                                                                                                                                                                |
| <b>Description</b>                     | A description of the software library.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Server Path</b>                     | <p>The software library path where the downloaded files are stored.</p> <p> <b>Note:</b></p> <p>The server path must not contain white spaces. For example, /user/mydownload is valid and /user/my download is invalid.</p>                                                                                                                                         |
| <b>Default Library</b>                 | An option to use a library as the default library when you download the firmware files.                                                                                                                                                                                                                                                                                                                                                                |
| <b>Default Protocol</b>                | <p>The default protocol for the software library where you download the firmware files. The options are:</p> <ul style="list-style-type: none"> <li>• <b>FTP</b></li> <li>• <b>SCP</b></li> <li>• <b>SFTP</b></li> </ul> <p> <b>Note:</b></p> <p>When you select the library on the File Download Manager page, the associated protocol is selected by default.</p> |

### SCP Configuration (S)

Use the SCP configuration to configure the SCP protocol details for the software library.

| Name                    | Description                                                                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable SCP</b>       | An option to enable the SCP configuration.<br>For this release, the <b>Enable SCP</b> option is selected by default. You cannot clear the selection. |
| <b>User Name</b>        | The user name for the SCP configuration.                                                                                                             |
| <b>Password</b>         | The password for the SCP configuration.                                                                                                              |
| <b>Confirm Password</b> | The password that you retype for the SCP configuration.                                                                                              |

### SFTP Configuration (T)

Use the SFTP configuration to configure the SFTP protocol details for the software library.

| Name                    | Description                                            |
|-------------------------|--------------------------------------------------------|
| <b>Enable SFTP</b>      | An option to enable the SFTP configuration.            |
| <b>User Name</b>        | The user name for the SFTP configuration.              |
| <b>Password</b>         | The password that you type for the SFTP configuration. |
| <b>Confirm Password</b> | The password that you retype for the SFTP password.    |

### FTP Configuration (F)

Use the FTP configuration to configure the FTP protocol details for the software library.

| Name                    | Description                                           |
|-------------------------|-------------------------------------------------------|
| <b>Enable FTP</b>       | An option to enable the FTP configuration.            |
| <b>User Name</b>        | The user name for the FTP configuration.              |
| <b>Password</b>         | The password that you type for the FTP configuration. |
| <b>Confirm Password</b> | The password that you retype for the FTP password.    |

### HTTP/HTTPS Configuration (H)

Use the HTTP/HTTPS configuration to configure the HTTP/HTTPS protocol details for the software library.

| Name                     | Description                                               |
|--------------------------|-----------------------------------------------------------|
| <b>Enable HTTP/HTTPS</b> | An option to enable the HTTP/HTTPS configuration.         |
| <b>URL</b>               | The software library URL.                                 |
| <b>User Name</b>         | The user name for the HTTP/HTTPS configuration.           |
| <b>Password</b>          | The password for the HTTP/HTTPS configuration.            |
| <b>Confirm Password</b>  | The password that you retype for the HTTP/HTTPS password. |

| Button                     | Description                                           |
|----------------------------|-------------------------------------------------------|
| <b>Commit</b>              | Saves the value you enter for the software library.   |
| <b>Clear Configuration</b> | Clears all entries you make, and resets the page.     |
| <b>Cancel</b>              | Cancels your action and returns to the previous page. |

---

## Viewing a file in the software library

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the Software Library Files page select the file that you want to view.
5. Click **View**.

You can view the details of the file in the View File page.

---

## Downloading the OVA file to System Manager

### About this task

You can download the software from Avaya PLDS or from an alternate source to System Manager. Use the procedure to download the OVA files to your computer and upload the file to System Manager.

### Before you begin

Set the local software library.

### Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services > Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
  - a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
  - b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
  - c. Click **Download**.

The system displays the Upload File page.

5. In the **Software Library** field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click **Browse** and select the OVA file from the location on the system.
8. Provide a valid file type.

This system uploads the OVA file from local computer to the designated software library on System Manager.

 **Note:**

If the file type is invalid, System Manager displays an error.

---

## Uploading a file to the software library

### About this task

Use the procedure to upload software files, such as OVA, images, and firmware that are required during the deployment, migration, upgrade, and update of Avaya Aura® applications.

### Before you begin

- On the Download Management page, click **Refresh Families**.
- When you add or update details in the application-specific `versions.xml` file, click **Refresh Families** again to get the updated information.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the System Manager command line interface, copy the required OVA file to the `/swlibrary/staging/sync/` location that you had created in System Manager.

 **Note:**

You require admin privileges to access the `/swlibrary/staging/sync/` location.

The system displays the file that you copied in the Sync Files from directory section.

5. Provide the following information:
  - **SHA256 Checksum:** The value mentioned in the source or original location of the file.
  - **Software Library:** The local or remote software library.
  - **Product Family**

 **Note:**

For SAL, in **Product Family**, **Device Type**, and **Software Type** fields, select **Others**.

- **Device Type**
- **Software Type**

If the file is already in `versions.xml`, the system populates the information.

If the file does not exist in `versions.xml`, the system does not display the file details. Therefore, you cannot use the file for upgrade in Upgrade Management. You can use the file only for new deployment from Application Management.

6. Select the file.

7. Click **Sync**.

In File Sync Started Message, the system displays the status of the schedule of the job.

8. Click **OK**.

When the job completes, the system displays the file in the Software Library Files section.

9. To check the status of the job, click **Services > Scheduler > Pending Jobs**.

When the job is complete, the system displays the file in the Software Library Files area and removes from Sync Files from directory.

---

## Deleting a file from the software library

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Software Library Management**.
3. Click **Manage Files**.
4. On the Software Library Files page, select the file or files you want to delete.
5. Click **Delete**.
6. On the confirmation page, click **Delete**.

---

## Software Library Files field descriptions

| Name                          | Description                                                                                                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b>              | The software file that you upload from your local directory to the selected library.                                                                        |
| <b>Device Type</b>            | The device type that you want to upgrade using the software library file. For example, CM_Duplex and CM_Simplex are device types for Communication Manager. |
| <b>Software Type</b>          | The type of software file that includes OVA file, firmware, and images.                                                                                     |
| <b>Version</b>                | The software file version that you want to upload.                                                                                                          |
| <b>Hardware Compatibility</b> | The hardware compatibility for the file you upload. For IP Office, this field can be blank.                                                                 |
| <b>File Length</b>            | The file length of the software file.                                                                                                                       |
| <b>Software Library</b>       | The software library where the file is created.                                                                                                             |

| Name                    | Description                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b>        | The software file that you upload from your local directory to the selected library.                                                       |
| <b>SHA256 Checksum</b>  | The sha256 checksum value of the file that you upload as mentioned in the source location of the file.                                     |
| <b>Software Library</b> | The software library where the file is created.                                                                                            |
| <b>Product Family</b>   | The product family to which the file belongs. In a product family, the number of devices are listed.                                       |
| <b>Device Type</b>      | The device type that you can upgrade using the software library file. For example, B5800 and IP Office are the device types for IP Office. |
| <b>Software Type</b>    | The type of software file which includes firmware and images.                                                                              |

| Button        | Description                                                                                 |
|---------------|---------------------------------------------------------------------------------------------|
| <b>View</b>   | Displays the file details page where you can view the details of the software library file. |
| <b>Delete</b> | Displays the Delete Software Files Confirmation page.                                       |
| <b>Done</b>   | Saves your action and returns to the previous page.                                         |

## System requirements for the external server

| Component                                                                                                          | Requirement                                                  | Recommendation                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Operating System                                                                                                   | Any standalone or virtualized Windows or Linux Distribution. |                                                                                                                    |
| Hard Drive                                                                                                         | 20–GB free space                                             | Ensure that the hard drive has enough free space to store the firmware files.                                      |
| Memory                                                                                                             | 2GB                                                          | As required by the operating system and the supported protocol services.                                           |
| Protocols: for the devices to download files from the external server                                              | FTP, SCP, SFTP, or HTTP service                              | Any supported HTTP server installation.<br><br>* <b>Note:</b><br>Currently, System Manager does not support HTTPS. |
| Protocols: for downloading the firmware upgrade files to the external server from PLDS site through System Manager | An FTP, SCP, or an SFTP server running on default ports      | Use SFTP or SCP for secure file transfer.                                                                          |



---

# Applications pre-upgrade functions

---

## Refreshing elements

### Before you begin

- On the User Settings page, configure the user settings.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
  - a. Select one or more devices.
  - b. Click **Pre-upgrade Actions > Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
  - **Run Immediately**: To perform the job.
  - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

The **Last Action Status** column displays  and the **Current Version** column displays the current version of the element.

---

## Analyzing software

### About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

### Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.

3. On the Upgrade Management page, do the following:
  - a. Select a device that you want to analyze.
  - b. Click **Pre-upgrade Actions > Analyze**.
4. On the Job Schedule page, click one of the following:
  - **Run Immediately**: To perform the job.
  - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

The **Last Action Status** column displays a , the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

---

## Downloading the software

### About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, select an element from the list.
4. In the left navigation pane, click **Download Management**.

The system displays the File Download Manager page.

5. To change the display settings, click one of the following:
  - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
  - **List View**: To view the list of elements in the list format. Every element is displayed individually.
6. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
7. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

The time to complete the refresh operation depends on the source configuration in **User Settings**.

8. Click **Show Files**.

9. In **Select Files Download Details**, do the following:

- a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.
- b. Select the files that you want to download.
- c. Click **Download**.

In File Download Status, the system displays the file that you selected for download.

## File Download Manager field descriptions

### Select Software/Hardware Types

| Name                     | Description                                      |
|--------------------------|--------------------------------------------------|
| <b>Family Name</b>       | The name of the device family.                   |
| <b>Hardware/Software</b> | The name of the associated software or hardware. |

### Select Files Download Details

| Name          | Description                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b> | The source from where Download Manager gets the software or firmware files. The options are: <ul style="list-style-type: none"> <li>• <b>Avaya PLDS/Alternate Source</b></li> <li>• <b>My Computer</b></li> </ul> |

| Name                        | Description                                  |
|-----------------------------|----------------------------------------------|
| <b>File name</b>            | The file name.                               |
| <b>Version</b>              | The file version.                            |
| <b>Entitled</b>             | The file entitlements.                       |
| <b>File Size (in bytes)</b> | The file size in bytes.                      |
| <b>Hardware/Software</b>    | The name of the hardware or the software.    |
| <b>Family Name</b>          | The name of the device family.               |
| <b>Content Type</b>         | The type of the content.                     |
| <b>Software Library</b>     | The status of the file download.             |
| <b>File Description</b>     | A description of the file that you download. |

| Button                  | Description                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Refresh Families</b> | Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page.<br><br>* <b>Note:</b><br>When you add or update details in the <code>versions.xml</code> file, you must click <b>Refresh Families</b> to get the updated information. |
| <b>Show Files</b>       | Displays the files associated with the element that you selected.                                                                                                                                                                                                                                                                                           |

### File Download Status

| Name                        | Description                                     |
|-----------------------------|-------------------------------------------------|
| <b>File Name</b>            | The file name of the software or firmware file. |
| <b>Job Name</b>             | The name of the download job.                   |
| <b>Current Step</b>         | The current status.                             |
| <b>Percentage Completed</b> | The status of completion.                       |
| <b>Status</b>               | The status of the download activity.            |
| <b>Scheduled By</b>         | The user who scheduled the download job.        |

| Button        | Description                               |
|---------------|-------------------------------------------|
| <b>Delete</b> | Deletes the files that you have selected. |

## Performing the preupgrade check

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
  - a. Select an application to upgrade.
  - b. Click **Pre-upgrade Actions > Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

\* **Note:**

To upgrade to different server, in **Target Host**, select the target server host.

5. On the Job Schedule page, click one of the following:
  - **Run Immediately:** To perform the job.
  - **Schedule later:** To perform the job at a scheduled time.
6. Click **Schedule**.

On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a .

## Preupgrade Configuration field descriptions

### Pre upgrade Configuration Parameters

| Name                       | Description                                                                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Element name</b>        | The name of the application that you want to upgrade.                                                                                                                                                                           |
| <b>Parent name</b>         | The parent of the application that you want to upgrade.                                                                                                                                                                         |
| <b>IP Address</b>          | The IP address of the application that you want to upgrade.                                                                                                                                                                     |
| <b>Current Version</b>     | The current version of the application that you want to upgrade.                                                                                                                                                                |
| <b>Target Platform</b>     | The Appliance Virtualization Platform or ESXi host of the virtual machine.                                                                                                                                                      |
| <b>Data Store</b>          | The data store.<br><br>When you set the <b>Target Host</b> as <b>Same Box</b> , the system enables the <b>Data Store</b> field.                                                                                                 |
| <b>New Target Platform</b> | The Appliance Virtualization Platform or ESXi host to which you want to upgrade the virtual machine.<br><br>For upgrades on a different server, add Appliance Virtualization Platform or ESXi host from Application Management. |
| <b>Upgrade Source</b>      | The location where OVA or the software patches are available in the local storage or remote server.                                                                                                                             |
| <b>Upgrade/Update To</b>   | The OVA file or the software patch to which you want to upgrade.                                                                                                                                                                |
| <b>Flexi Footprint</b>     | The file based on the storage, CPU, and memory capacity of your system.                                                                                                                                                         |

### Job Schedule

| Name                | Description                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Job</b> | The option to schedule a job: <ul style="list-style-type: none"> <li>• <b>Run immediately</b>: To run the upgrade job immediately.</li> <li>• <b>Schedule later</b>: To run the upgrade job at the specified date and time.</li> </ul> |
| <b>Date</b>         | The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.                |

*Table continues...*

| Name             | Description                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time</b>      | The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job. |
| <b>Time Zone</b> | The time zone of your region.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.                                                                           |

| Name            | Description                                                                       |
|-----------------|-----------------------------------------------------------------------------------|
| <b>Schedule</b> | Runs the job or schedules to run at the time that you configured in Job Schedule. |

---

## Application management

---

### Application management

The Application Management link from Solution Deployment Manager provides the application management capabilities that you can use to do the following.

- Defines the physical location, Avaya Aura® Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Supports password change and patch installation of the Avaya Aura® Appliance Virtualization Platform host. Restart, shutdown, and certificate validation of Appliance Virtualization Platform and ESXi hosts. Also, enables and disables SSH on the host.
- Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance Virtualization Platform or ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.

 **Note:**

For the Avaya Aura® Messaging element, trust re-establishment is not required.

- Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and Avaya Aura® Virtualized Appliance environment.
- Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- Deploys Avaya Aura® application ISOs in Software-only environment.
- Configures application and networking parameters required for application deployments.
- Supports flexible footprint definition based on capacity required for the deployment of the Avaya Aura® application OVA.

You can deploy the OVA or ISO file on the platform by using System Manager Solution Deployment Manager or the Solution Deployment Manager client.

---

## Managing the location

### Viewing a location

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click the Locations tab.

The Locations section lists all locations.

### Adding a location

#### About this task

You can define the physical location of the host and configure the location specific information. You can update the information later.

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the **Locations** tab, in the Locations section, click **New**.
3. In the New Location section, perform the following:
  - a. In the Required Location Information section, type the location information.
  - b. In the Optional Location Information section, type the network parameters for the virtual machine.
4. Click **Save**.

The system displays the new location in the **Application Management Tree** section.

#### Related links

[New and Edit location field descriptions](#) on page 1318

### Editing the location

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the **Locations** tab, in the Locations section, select a location that you want to edit.
3. Click **Edit**.
4. In the Edit Location section, make the required changes.

5. Click **Save**.

## Related links

[New and Edit location field descriptions](#) on page 1318

## Deleting a location

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the **Locations** tab, in the Locations section, select one or more locations that you want to delete.
3. Click **Delete**.
4. In the Delete confirmation dialog box, click **Yes**.

The system does not delete the applications that are running on the platform and moves the platform to **Unknown location Platform mapping**.

## New and Edit location field descriptions

### Required Location Information

| Name                         | Description                                                                         |
|------------------------------|-------------------------------------------------------------------------------------|
| <b>Name</b>                  | The location name.                                                                  |
| <b>Avaya Sold-To #</b>       | The customer contact number.<br>Administrators use the field to check entitlements. |
| <b>Address</b>               | The address where the host is located.                                              |
| <b>City</b>                  | The city where the host is located.                                                 |
| <b>State/Province/Region</b> | The state, province, or region where the host is located.                           |
| <b>Zip/Postal Code</b>       | The zip code of the host location.                                                  |
| <b>Country</b>               | The country where the host is located.                                              |

### Optional Location Information

| Name                   | Description                                                                             |
|------------------------|-----------------------------------------------------------------------------------------|
| <b>Default Gateway</b> | The IP address of the virtual machine gateway. For example, 172.16.1.1.                 |
| <b>DNS Search List</b> | The search list of domain names.                                                        |
| <b>DNS Server 1</b>    | The DNS IP address of the primary virtual machine. For example, 172.16.1.2.             |
| <b>DNS Server 2</b>    | The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.           |
| <b>NetMask</b>         | The subnet mask of the virtual machine.                                                 |
| <b>NTP Server</b>      | The IP address or FQDN of the NTP server.<br>Separate the IP addresses with commas (,). |



| Button        | Description                                                                           |
|---------------|---------------------------------------------------------------------------------------|
| <b>Save</b>   | Saves the location information and returns to the Locations section.                  |
| <b>Edit</b>   | Updates the location information and returns to the Locations section.                |
| <b>Delete</b> | Deletes the location information, and moves the host to the Unknown location section. |
| <b>Cancel</b> | Cancels the add or edit operations, and returns to the Locations section.             |

## Managing the platform

### Adding an Appliance Virtualization Platform or ESXi host

#### About this task

Use the procedure to add an Appliance Virtualization Platform or ESXi host. You can associate an ESXi host with an existing location.

If you are adding a standalone ESXi host to System Manager Solution Deployment Manager or to the Solution Deployment Manager client, add the standalone ESXi host using its FQDN only.

#### **Note:**

You can add a VMware ESXi host in Solution Deployment Manager only if Standard or Enterprise VMware license is applied on the VMware ESXi host.

If VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or VMware ESXi host is in evaluation period, you cannot add that VMware ESXi host in Solution Deployment Manager.

Solution Deployment Manager only supports the Avaya Aura® Appliance Virtualization Platform and VMware ESXi hosts. If you try to add another host, the system displays the following error message:

```
Retrieving host certificate info is failed: Unable to communicate with
host. Connection timed out: connect. Solution Deployment Manager only
supports host management of VMware-based hosts and Avaya Appliance
Virtualization Platform (AVP).
```

#### Before you begin

Add a location.

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.

5. In the New Platform section, do the following:

- a. Provide details of Platform name, Platform FQDN or IP address, user name, and password.

For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root user name.

- b. In **Platform Type**, select **AVP/ESXi**.
- c. If you are connected through the services port, set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6.

6. Click **Save**.

7. In the Certificate dialog box, click **Accept Certificate**.

The system generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can only accept the certificate. If the certificate is invalid, Solution Deployment Manager displays the error. To generate certificate, see VMware documentation.

In the Application Management Tree section, the system displays the new host in the specified location. The system also discovers applications.

8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:

- a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
- b. Click **More Actions > Re-establish connection**.  
For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
- c. Click **More Actions > Refresh App**.

 **Important:**

When you change the IP address or FQDN of the Appliance Virtualization Platform host from the local inventory, you require AVP Utilities. To get the AVP Utilities application name during the IP address or FQDN change, refresh AVP Utilities to ensure that AVP Utilities is available.

9. On the **Platforms** tab, select the required platform and click **Refresh**.

## Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element > Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines that are deployed on the host.
2. Ensure that the system populates the **Application Name** and **Application Version** for each virtual machine.

## Related links

[Add and Edit platform field descriptions](#) on page 1343

## Adding a software-only platform

### About this task

Use this procedure to add an operating system on Solution Deployment Manager. In Release 8.1.3, the system supports the Red Hat Enterprise Linux Release 7.6 64-bit operating system.

 **Note:**

### Before you begin

Add a location.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the **Platforms** tab, click **Add**.
3. In **Platform Name**, type the name of the platform.
4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.
5. In **User Name**, type the user name of the base operating system.

For a software-only deployment, the user name must be a direct access admin user. If the software-only application is already deployed, provide the application cli user credentials.

6. In **Password**, type the password of the base operating system.
7. In **Platform Type**, select **OS**.
8. Click **Save**.

If the platform has some applications running, the system automatically discovers those applications and displays the applications in the **Applications** tab.

- If Solution Deployment Manager is unable to establish trust, the system displays the application as Unknown.
- If you are adding OS, only **Add** and **Remove** operations are available on the **Platforms** tab. You cannot perform any other operations. On the **Applications** tab, the system enables the **New** option. If the application is System Manager, the system enables **Update App** on Solution Deployment Manager Client

The system displays the added base operating system on the **Platforms** tab.

## Editing a platform

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select a platform that you want to update.
4. Change the platform information.
5. Click **Save**.

The system updates the platform information.

#### Related links

[Add and Edit platform field descriptions](#) on page 1343

## Rolling back to Utility Services

### About this task

Use this procedure to rollback Utility Services to 7.x if the upgrade from Utility Services to AVP Utilities fails from Release 7.x to Release 8.1 and later.

### Before you begin

- Add a location.
- Select Location and add a host.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location<location name> section, select the Utility Services application, and click **More Actions > Rollback/Retry**.

If the **Current Action Status** column displays the VM Upgrade Failed message, the system enables **More Actions > Rollback/Retry** after selecting the Utility Services application.

4. In the Import Configuration Excel File dialog box, click **Rollback**.

To upgrade Utility Services to AVP Utilities, use the Upgrade Management page of System Manager Solution Deployment Manager.

The system displays the confirmation message to accept the rollback.

## Retrying Utility Services to AVP Utilities upgrade

### About this task

If the upgrade from Utility Services to AVP Utilities fails, use this procedure to retry the upgrade of Utility Services to AVP Utilities.

### Before you begin

- Add a location.

- Select Location and add a host.
- Download a copy of the `hostUSUpgradeInfo.xlsx` spreadsheet from Avaya PLDS website at <https://plds.avaya.com/> or from Avaya Support website at <https://support.avaya.com>. Fill the required system details in the spreadsheet.

 **Note:**

If you provide the incorrect data in the spreadsheet, the upgrade might fail.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location<location name> section, select the Utility Services application, and click **More Actions > Rollback/Retry**.

If the **Current Action Status** column displays the `VM Upgrade Failed` message, the system enables **More Actions > Rollback/Retry** after selecting the Utility Services application.

4. On the Import Configuration Excel File dialog box, do the following:

- a. Click **Browse** and select the file from the local computer.
- b. To upload the spreadsheet, click **Open**.

The system displays the file size and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.

- c. Click **Submit File**.

Once the file is successfully uploaded, the system enables the **Retry** button.

- d. Click **Retry**.

The system starts the upgrade of Utility Services to AVP Utilities.

## Changing the network parameters for an Appliance Virtualization Platform host

### About this task

Use this procedure to change the network parameters of Appliance Virtualization Platform after deployment. You can change network parameters only for the Appliance Virtualization Platform host.

 **Note:**

If you are connecting to Appliance Virtualization Platform through the public management interface, you might lose connection during the process. Therefore, after the IP address changes, close Solution Deployment Manager, and restart Solution Deployment Manager by using the new IP address .

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host and click **Change Network Params > Change Host IP Settings**.
4. In the Host Network/ IP Settings section, change the IP address, subnet mask, and other parameters as appropriate.

### **Note:**

An Avaya Aura® Appliance Virtualization Platform host and all virtual machines running on the host must be on the same subnet mask.

If Out of Band Management is configured in an Avaya Aura® Appliance Virtualization Platform deployment, you need two subnet masks, one for each of the following:

- Public or signaling traffic, Avaya Aura® Appliance Virtualization Platform, and all virtual machines public traffic.
- Management, Avaya Aura® Appliance Virtualization Platform, and all virtual machine management ports.

5. To change the gateway IP address, do the following:
  - a. Click **Change Gateway**.  
The **Gateway** field becomes available for providing the IP address.
  - b. In **Gateway**, change the IP address.
  - c. Click **Save Gateway**.
6. Click **Save**.  
The system updates the Appliance Virtualization Platform host information.

## Related links

[Change Network Parameters field descriptions](#) on page 1344

## Changing the network settings for an Appliance Virtualization Platform host from Solution Deployment Manager

### About this task

With Appliance Virtualization Platform, you can team NICs together to provide a backup connection when the server NIC or the Ethernet switch fails. You can also perform NIC teaming from the command line on Appliance Virtualization Platform.

Appliance Virtualization Platform supports Active-Standby and Active-Active modes of NIC teaming. For more information, see “NIC teaming modes”.

**\* Note:**

- If you add a host with service port IP address in Solution Deployment Manager and change the IP address of the host to the public IP address by using Host Network/ IP Settings, the system updates the public IP address in the database. Any further operations that you perform on the host fail because the public IP address cannot be reached with the service port. To avoid this error, edit the host with the service port IP address again.
- If FQDN of the Appliance Virtualization Platform host is updated by using Host Network/IP setting for domain name, refresh the host so that the FQDN changes reflect in Solution Deployment Manager.

Use this procedure to change network settings, such as changing VLAN ID, NIC speed, and manage NIC team for an Appliance Virtualization Platform host.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **Change Network params > Change Network Settings**.

Host Network/IP Settings ( 172.19.72.137 )

Out Of Band Management for host: **disabled**    Server Model: **ProLiant DL360 Gen9**    No. of Switches: **3**

Standard Switches    Advanced Configuration

**vSwitch0 (Public and Management Traffic)**

| PortGroups                                   | NICs                                                                                                                                                                                   |             |       |             |        |           |  |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------|-------------|--------|-----------|--|
| Management Network (  VLANID : None (0))     | Change NIC speed    NIC team/unteam                                                                                                                                                    |             |       |             |        |           |  |
| Out of Band Management (  VLANID : None (0)) | <table border="1"> <thead> <tr> <th>NIC Name</th> <th>Speed</th> <th>Link Status</th> </tr> </thead> <tbody> <tr> <td>vmnic0</td> <td>100, Full</td> <td></td> </tr> </tbody> </table> | NIC Name    | Speed | Link Status | vmnic0 | 100, Full |  |
| NIC Name                                     | Speed                                                                                                                                                                                  | Link Status |       |             |        |           |  |
| vmnic0                                       | 100, Full                                                                                                                                                                              |             |       |             |        |           |  |
| Public (  VLANID : None (0))                 |                                                                                                                                                                                        |             |       |             |        |           |  |
| 1 virtual machine(s)                         |                                                                                                                                                                                        |             |       |             |        |           |  |
| avp72vm138                                   |                                                                                                                                                                                        |             |       |             |        |           |  |

Cancel

The Host Network/ IP Settings page displays the number of switches as 4.

You can configure port groups for the following switches:

- **vSwitch0**, reserved for the Public and Management traffic.
- **vSwitch1**, reserved for services port. You cannot change the values.

- **vSwitch2**, reserved for Out of Band Management.
- **vSwitch3**. No reservations.
- **vSwitch4**. No reservations.
- **vSwitch5**. No reservations.

5. To change VLAN ID, click **Standard Switches**, and perform the following:

- a. Expand the vSwitch<n> section by clicking the downward arrow .

The section displays the vSwitch details.

- b. Click on the VLANID link or the edit icon ().

The system displays the Port Group Properties page where you can edit the VLAN ID port group property.

- c. In **VLAN ID**, select an ID.

For more information about the value, see NIC teaming.

- d. Click **OK**.

The system displays the new VLAN ID.

6. To change the NIC speed, click **Standard Switches**, and perform the following:

- a. Ensure that the system displays a vmnic in the **NIC Name** column.

- b. Click **Change NIC speed**.

The system displays the selected vmnic dialog box.

- c. In **Configured speed, Duplex**, click a value.

- d. Click **OK**.

For more information, see VLAN ID assignment.

The system displays the updated NIC speed in the **Speed** column.

If the NIC is connected, the system displays a check mark  in **Link Status**.

 **Note:**

You can change the speed only for common servers. You cannot change the speed for the S8300E server.

7. To change the NIC teaming, click **Standard Switches**, and perform the following:

- a. Select a vmnic.

- b. Click **NIC team/unteam**.

The system displays the Out of Band Management Properties page.

- c. To perform NIC teaming or unteaming, select the vmnic, and click **Move Up** or **Move Down** to move the vmnic from **Active Adapters**, **Standby Adapters**, or **Unused Adapters**.



For more information, see “NIC teaming modes”.

- d. Click **OK**.

The vmnic teams or unteams with **Active Adapters**, **Standby Adapters**, or **Unused Adapters** as required.

- e. To check the status of the vmnic, click **NIC team/unteam**.

8. To get the latest data on the host network IP settings, click **Refresh** .

The system displays the current status of the vmnic.

 **Note:**

You cannot perform NIC teaming for the S8300E server.

### Related links

[Host Network / IP Settings field descriptions](#) on page 1345

## Deleting the unused port

### About this task

Use this procedure to delete the unused port of Solution Deployment Manager that is no longer used by applications that are deployed on an Appliance Virtualization Platform host.

For example, you can delete the unused port, if an application is deleted from the Appliance Virtualization Platform host, and the system still has those ports available on the Appliance Virtualization Platform host.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **Change Network params > Change Network Settings**.
5. Click **Advanced Configuration**.
6. In the Unused PortGroups section, select the portgroup.
7. Click **Delete**.

## Changing the password for an Appliance Virtualization Platform host

### About this task

Use this procedure to change the password for the Appliance Virtualization Platform host. This is the password for the administrator that you provide when deploying the Appliance Virtualization Platform host.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, do the following:
  - a. Select a host.
  - b. Click **More Actions > Change Password**.
4. In the Change Password section, type the current password and the new password.  
For more information about password rules, see “Password policy”.
5. Click **Change Password**.

The system updates the password of the Appliance Virtualization Platform host.

## Related links

[Password policy](#) on page 1328

[Change Password field descriptions](#) on page 1346

## Password policy

The password must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.
- Must not contain an uppercase letter at the beginning and a digit at the end.

### **Note:**

An Uppercase letter at the beginning of a password is not counted for the password complexity rule. The Uppercase letter must be within the password.

Example of a valid password is *myPassword\$*.

If the password does not meet the requirements, the system prompts you to enter a new password. Enter the existing password and the new password in the correct fields.

Ensure that you keep the admin password safe. You need the password while adding the host to Solution Deployment Manager and for troubleshooting.

## Related links

[Changing the password for an Appliance Virtualization Platform host](#) on page 1327

## Generating the Appliance Virtualization Platform kickstart file

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. In the lower pane, click **Generate AVP Kickstart**.

3. On Create AVP Kickstart, do the following:

- a. Select **8.1.x**.
- b. Enter the appropriate information in the fields.
- c. Click **Generate Kickstart File**.

For more information, see “Create AVP Kickstart field descriptions.”

The system prompts you to save the generated kickstart file on your local computer.

For Appliance Virtualization Platform Release 8.1 and later, the kickstart file name must be `avp81ks.cfg`.

## Related links

[Create AVP Kickstart field descriptions](#) on page 1329

## Create AVP Kickstart field descriptions

| Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Choose AVP Version</b>                    | The field to select the release version of Appliance Virtualization Platform.                                                                                                                                                                                                                                                                                                                 |
| <b>Dual Stack Setup (with IPv4 and IPv6)</b> | Enables or disables the fields to provide the IPv6 addresses.<br>The options are: <ul style="list-style-type: none"> <li>• <b>yes</b>: To enable the IPv6 format.</li> <li>• <b>no</b>: To disable the IPv6 format.</li> </ul>                                                                                                                                                                |
| <b>AVP Management IPv4 Address</b>           | IPv4 address for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                  |
| <b>AVP IPv4 Netmask</b>                      | IPv4 subnet mask for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                              |
| <b>AVP Gateway IPv4 Address</b>              | IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.                                                                                                                                                                                                                                                                              |
| <b>AVP Hostname</b>                          | Hostname for the Appliance Virtualization Platform host.<br>The hostname: <ul style="list-style-type: none"> <li>• Can contain alphanumeric characters and hyphen</li> <li>• Can start with an alphabetic or numeric character</li> <li>• Must contain at least 1 alphabetic character</li> <li>• Must end in an alphanumeric character</li> <li>• Must contain 1 to 63 characters</li> </ul> |
| <b>AVP Domain</b>                            | Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.                                                                                                                                                                                                  |
| <b>IPv4 NTP server</b>                       | IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com                                                                                                                                                                                                                                                                                                           |

*Table continues...*

| Name                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secondary IPv4 NTP Server</b>            | Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Main IPv4 DNS Server</b>                 | Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Secondary IPv4 DNS server</b>            | Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>AVP management IPv6 address</b>          | IPv6 address for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>AVP IPv6 prefix length</b>               | IPv6 subnet mask for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>AVP gateway IPv6 address</b>             | IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>IPv6 NTP server</b>                      | IPv6 address or FQDN of customer NTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Secondary IPv6 NTP server</b>            | Secondary IPv6 address or FQDN of customer NTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Main IPv6 DNS server</b>                 | Main IPv6 address of customer DNS server. One DNS server entry in each line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Secondary IPv6 DNS server</b>            | Secondary IPv6 address of customer DNS server. One DNS server entry in each line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Public vLAN ID (Used on S8300E only)</b> | VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090.<br><br>Use <b>Public VLAN ID</b> only on the S8300E server.                                                                                                                                                                                                                                                                                                                                      |
| <b>Out of Band Management Setup</b>         | The check box to enable or disable Out of Band Management for Appliance Virtualization Platform. If selected the management port connects to eth2 of the server, and applications can deploy in the Out of Band Management mode.<br><br>The options are:<br><ul style="list-style-type: none"> <li>• <b>yes</b>: To enable Out of Band Management<br/>The management port is connected to eth2 of the server, and applications can deploy in the Out of Band Management mode.</li> <li>• <b>no</b>: To disable Out of Band Management. The default option.</li> </ul> |
| <b>OOBM vLAN ID (Used on S8300E only)</b>   | <ul style="list-style-type: none"> <li>• For S8300E, use the front plate port for Out of Band Management</li> <li>• For common server, use eth2 for Out of Band Management.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |
| <b>AVP Super User Admin Password</b>        | Admin password for Appliance Virtualization Platform.<br><br>The password must contain at least 8 characters and can include alphanumeric characters and @!\$.<br><br>You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.                                                                                                                                                                                                                                                 |
| <b>Confirm Password</b>                     | Admin password for Appliance Virtualization Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Table continues...

| Name                                                  | Description                                                                                                                                                                                   |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Stricter Password (14 char pass length)</b> | The check box to enable or disable the stricter password.<br>The password must contain at least 14 characters.                                                                                |
| <b>Validity in Days (Used on AVP Certificate)</b>     | The number of days for the Appliance Virtualization Platform certificate validation. The maximum limit for the certificate validation is 825 days. You can configure from 1 through 825 days. |
| <b>WebLM IP/FQDN</b>                                  | The IP Address or FQDN of WebLM Server.                                                                                                                                                       |
| <b>WebLM Port Number</b>                              | The port number of WebLM Server. The default port is 52233.                                                                                                                                   |

| Button                         | Description                                                                                                                        |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generate Kickstart File</b> | Generates the Appliance Virtualization Platform kickstart file and the system prompts you to save the file on your local computer. |

### Related links

[Generating the Appliance Virtualization Platform kickstart file](#) on page 1328

## Enabling and disabling SSH on Appliance Virtualization Platform from Solution Deployment Manager

### About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. To continue access, enable the SSH service on Appliance Virtualization Platform from Solution Deployment Manager.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. Select an Appliance Virtualization Platform host.
4. To enable SSH, do the following:
  - a. Click **More Actions > SSH > Enable SSH**.
  - b. In the Confirm dialog box, in the **Time (in minutes)** field, type the time after which the system times out the SSH connection.  
The range is 10 minutes through 120 minutes.
  - c. Click **Ok**.  
The system displays `enabled` in the **SSH status** column.
5. To disable SSH, click **More Actions > SSH > Disable SSH**.  
The system displays `disabled` in the **SSH status** column.

## Activating SSH from AVP Utilities

### About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must activate SSH on Appliance Virtualization Platform.

When you install or preinstall Appliance Virtualization Platform on a server, SSH is enabled. After you accept the license terms during Appliance Virtualization Platform installation, SSH shuts down within 24 hours. After SSH shuts down, you must reactivate SSH by using the **AVP\_SSH enable** command from AVP Utilities.

### Before you begin

Start an SSH session.

### Procedure

1. Log in to the AVP Utilities virtual machine running on Appliance Virtualization Platform with administrator privilege credentials.
2. Type the following:

```
AVP_SSH enable
```

Within 3 minutes, from AVP Utilities, the SSH service starts on Appliance Virtualization Platform and runs for two hours. After two hours, you must reactivate SSH from AVP Utilities.

When SSH is enabled, you can use an SSH client such as PuTTY to gain access to Appliance Virtualization Platform on customer management IP address or the services port IP address of 192.168.13.6.

3. **(Optional)** To find the status of SSH, type `AVP_SSH status`.
4. To disable SSH, type `AVP_SSH disable`.

## Enabling and disabling SSH on Appliance Virtualization Platform from System Manager CLI

### About this task

For security purpose, SSH access to Appliance Virtualization Platform shuts down in the normal operation. You must enable the SSH service on Appliance Virtualization Platform.

You can enable SSH, disable SSH, and check the SSH status on the Appliance Virtualization Platform host.

### Before you begin

Start an SSH session.

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Navigate to the `$MGMT_HOME/infra/bin/avpSSHUtility` location.

3. Type `./enableDisableSSHOnAVP.sh`.

The system displays the following options:

- Enable SSH on the Appliance Virtualization Platform host.
- Disable SSH on the Appliance Virtualization Platform host.
- Check the SSH status on the Appliance Virtualization Platform host.

4. To enable SSH, perform the following:

- a. At the prompt, type `1` and press `Enter`.
- b. Type the IP address of the Appliance Virtualization Platform host.
- c. Type the time in minutes.

The time is the duration after which the system blocks any new SSH connections. The valid range 10 to 120 minutes.

The system displays the message and enables SSH on Appliance Virtualization Platform host.

For example, if you set the time to 50 minutes, after 50 minutes, the system blocks any new SSH connections. If you reenables SSH before completion of 50 minutes, the system adds 50 minutes to the initial 50 minutes to reenables connections.

5. To disable SSH, perform the following:

- a. At the prompt, type `2` and press `Enter`.
- b. Type the IP address of the Appliance Virtualization Platform host.

If SSH is already disabled, the system displays `False` and the message `SSH is already disabled. No operation performed. Exiting.`

6. **(Optional)** To view the status of SSH, perform the following:

- a. At the prompt, type `3` and press `Enter`.
- b. Type the IP address of the Appliance Virtualization Platform host.

If SSH is enabled, the system displays `Is SSH enable - false`.

If SSH is disabled, the system displays `Is SSH disable - true`.

## Changing the IP address and default gateway of the host

### About this task

When you change the default gateway and IP address from the vSphere web client, the change might be unsuccessful.

You cannot remotely change the IP address of the Appliance Virtualization Platform host to a different network. You can change the IP address remotely only within the same network.

To change the Appliance Virtualization Platform host to a different network, perform Step 2 or Step 3.

## Before you begin

Connect the computer to the services port.

## Procedure

1. Start an SSH session.
2. Log in to the Appliance Virtualization Platform host command line interface with admin user credentials.
3. At the command prompt of the host, do the following:

- a. To change the IP address, type the following:

```
esxcli network ip interface ipv4 set -i vmk0 -I <old IP address of the host> -N <new IP address of the host> -t static
```

For example:

```
esxcli network ip interface ipv4 set -i vmk0 -I 135.27.162.121 -N 255.255.255.0 -t static
```

- b. To change the default gateway, type `esxcfg-route <new gateway IP address>`.

For example:

```
esxcfg-route 135.27.162.1
```

4. Enable SSH on Appliance Virtualization Platform and run the `/opt/avaya/bin/./serverInitialNetworkConfig` command.

For more information, see Configuring servers preinstalled with Appliance Virtualization Platform.

## Appliance Virtualization Platform license

From Appliance Virtualization Platform Release 7.1.2, you must install an applicable Appliance Virtualization Platform host license file on an associated Avaya WebLM server and configure Appliance Virtualization Platform to obtain its license from the WebLM server. WebLM Server can be either embedded System Manager WebLM Server or standalone WebLM Server. Appliance Virtualization Platform licenses are according to the supported server types.

For information about Appliance Virtualization Platform licenses and supported server types, see “Appliance Virtualization Platform licenses for supported servers”.

To configure the Appliance Virtualization Platform license file:

1. Obtain the applicable license file from the Avaya PLDS website.
2. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

### **Note:**

The Appliance Virtualization Platform license file can contain multiple Appliance Virtualization Platform licenses that is for four different server types. One Appliance



Virtualization Platform license file contains all the necessary licenses for the complete solution.

3. Configure the applicable **WebLM IP Address/FQDN** field for each Appliance Virtualization Platform host by using either System Manager Solution Deployment Manager, Solution Deployment Manager Client, or Appliance Virtualization Platform host command line interface.

You can view the license status of the Appliance Virtualization Platform host on the **Platforms** tab of the System Manager Solution Deployment Manager or Solution Deployment Manager Client interfaces. The Appliance Virtualization Platform license statuses on the **Platforms** tab are:

- **Normal:** If the Appliance Virtualization Platform host has acquired a license, the **License Status** column displays **Normal**.
- **Error:** If the Appliance Virtualization Platform host has not acquired a license. In this case, the Appliance Virtualization Platform enters the License Error mode and starts a 30-day grace period. The **License Status** column displays **Error - Grace period expires: <DD/MM/YY> <HH:MM>**.
- **Restricted:** If the 30-day grace period of the Appliance Virtualization Platform license expires, Appliance Virtualization Platform enters the License Restricted mode and restricts the administrative actions on the host and associated virtual machines. The **License Status** column displays **Restricted**. After you install a valid Appliance Virtualization Platform license on the configured WebLM Server, the system restores the full administrative functionality.

 **Note:**

Restricted administrative actions for:

- **AVP Host: AVP Update/Upgrade Management, Change Password, Host Shutdown, and AVP Cert. Management.**
- **Application: New, Delete, Start, Stop, and Update.**

### Appliance Virtualization Platform licensing alarms

If the Appliance Virtualization Platform license enters either License Error Mode or License Restricted Mode, the system generates a corresponding Appliance Virtualization Platform licensing alarm. You must configure the Appliance Virtualization Platform alarming. For information about how to configure the Appliance Virtualization Platform alarming feature, see *Administering Avaya Aura® AVP Utilities*.

## Configuring WebLM Server for an Appliance Virtualization Platform host using Solution Deployment Manager

### Before you begin

1. Add an Appliance Virtualization Platform host.  
For information about adding a host, see *Administering Avaya Aura® System Manager*.
2. Obtain the license file from the Avaya PLDS website.
3. Install the license file on the System Manager WebLM Server or Standalone WebLM Server.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section:
  - a. Select the Appliance Virtualization Platform host.
  - b. Click **More Actions > WebLM Configuration**.

The system displays the WebLM Configuration dialog box.

4. In **WebLM IP Address/FQDN**, type the IP address or FQDN of WebLM Server.

For WebLM configuration, if you select:

- Only one host then **WebLM IP Address/FQDN** displays the existing WebLM Server IP Address.
- Multiple hosts then **WebLM IP Address/FQDN** will be blank to assign the same WebLM Server IP Address for all the selected Appliance Virtualization Platform hosts.

5. In **Port Number**, type the port number of WebLM Server.

Embedded System Manager WebLM Server supports both 443 and 52233 ports.

6. Click **Submit**.

The system displays the status in the **Current Action** column.

The system takes approximately 9 minutes to acquire the Appliance Virtualization Platform host license file from the configured WebLM Server. On the **Platforms** tab, click **Refresh**.

When the Appliance Virtualization Platform host acquires the license, on the **Platforms** tab, the **License Status** column displays **Normal**.

## WebLM Configuration field descriptions

| Name                         | Description                                                 |
|------------------------------|-------------------------------------------------------------|
| <b>WebLM IP Address/FQDN</b> | The IP Address or FQDN of WebLM Server.                     |
| <b>Port Number</b>           | The port number of WebLM Server. The default port is 52233. |

| Button        | Description                                |
|---------------|--------------------------------------------|
| <b>Submit</b> | Saves the WebLM Server configuration.      |
| <b>Cancel</b> | Closes the WebLM Configuration dialog box. |

## Viewing the Appliance Virtualization Platform host license status using Solution Deployment Manager

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, view the Appliance Virtualization Platform host license status in the **License Status** column.

## Shutting down the Appliance Virtualization Platform host

### About this task

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions > Lifecycle Action > Host Shutdown**.

The Appliance Virtualization Platform host and virtual machines shut down.

## Restarting Appliance Virtualization Platform or an ESXi host

### About this task

The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Web Client or through the Solution Deployment Manager client.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions > Lifecycle Action > Host Restart**.
5. On the confirmation dialog box, click **Yes**.

The system restarts the host and virtual machines running on the host.

## Removing an Appliance Virtualization Platform or ESXi host

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
3. Click **Remove**.
4. On the Delete page, click **Yes**.

## Viewing Appliance Virtualization Platform firewall rules

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select an Appliance Virtualization Platform host, and click **More Actions > AVP Firewall Rules**.

System Manager displays the Firewall Settings page.

4. To view the additional details, select a row.

System Manager displays the details in the separate section on the Firewall Settings page.

## Configuring the login banner for the Appliance Virtualization Platform host

### About this task

You can configure a login banner message on one or more Appliance Virtualization Platform hosts at a time.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the Host tab, in Platforms for Selected Location <location name>, select one or more Appliance Virtualization Platform hosts on which you want to configure the message.
4. Click **More Actions > Push Login Banner**.

You can change the login banner text only on the Security Settings page from **Security > Policies** on System Manager.

5. On the Message of the Day window, click **Push Message**.

The system updates the login banner on the selected Appliance Virtualization Platform hosts.

## Mapping the ESXi host to an unknown location

### About this task

When you delete a location, the system does not delete the virtual machines running on the host, and moves the host to **Unknown location Platform mapping**. You can configure the location of an ESXi host again.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the left navigation pane, click the **Unknown location Platform mapping** link.
3. In the Host Location Mapping section, select an ESXi host, and click **Edit**.

The system displays the Host Information page.

4. Select a location and click **Update**.
5. Select the host(s) where location is updated and click **Submit**.

The system displays the ESXi host in the selected location.

## Applying third-party AVP certificates

### Applying third-party certificates to Appliance Virtualization Platform

#### About this task

Use this procedure to create, download, upload, and push third-party certificates to Appliance Virtualization Platform hosts.

#### Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.
- Ensure that the certificate on the Appliance Virtualization Platform host is valid.

#### Note:

If you are using a third-party generated CSR, add the private key for the CSR in the file `/etc/vmware/ssl/rui_csr_temp.key` before installing the certificate from Solution Deployment Manager.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. **(Optional)** Add the details of the generic CSR.

If you add the generic CSR details, the system pre-populates the values in the View/Generate CSR dialog box.

For more information about creating the generic CSR, see “Creating or editing generic CSR”.

5. To generate CSR, do the following:

- a. Click **More Actions > AVP Cert. Management > Manage Certificate**.
- b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
- c. Click **View/Generate CSR**.  
System Manager displays the View/Generate CSR dialog box.
- d. If the generic CSR details are not added for the Appliance Virtualization Platform host, add the details of the generic CSR.
- e. Click **Generate CSR**.  
The system generates CSR for the Appliance Virtualization Platform host.
- f. In the **Current Action** column, click **Status Details** to view the status.

6. To download CSR, do the following:

- a. Click **More Actions > AVP Cert. Management > Manage Certificate**.
- b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
- c. Click **Download CSR**.  
In case of Firefox browser, the system prompts you to save the CSR.zip file.
- d. In the **Current Action** column, click **Status Details** to view the status.  
In the Download CSR Status dialog box, the system displays the path of the downloaded CSR.zip file.

7. Extract the downloaded certificates, and ensure that the third-party signs them.

8. To upload and push the signed certificate from a third-party CA, do the following:

- a. Click **More Actions > AVP Cert. Management > Manage Certificate**.
- b. In the Load Certificate dialog box, select one or more Appliance Virtualization Platform hosts.
- c. Click **Browse** and select the required certificates from the local computer.
- d. Click **I Agree to accept to add the same certificate in SDM**.
- e. Click **Push Certificate**.
- f. In the **Current Action** column, click **Status Details** to view the status.

## Creating or editing generic CSR

### About this task

Use this procedure to create or edit a generic CSR for third-party Appliance Virtualization Platform certificates. With a generic CSR, you can apply the same set of data for more than one Appliance Virtualization Platform host.

### Procedure

1. In **Application Management Tree**, select a location.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
3. Click **More Actions > AVP Cert. Management > Generic CSR**.
4. In the Create/Edit CSR dialog box, add or edit the details of the generic CSR, such as organization, organization unit, locality, state, country, and email.
5. Click **Create/Edit CSR** and then click **OK**.

### Next steps

Complete the CSR generation, download, third-party signing and push the certificates to the Appliance Virtualization Platform hosts.

### Load Certificate field descriptions

| Name                                                         | Description                                                                                 |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Platform IP</b>                                           | The IP address of the Appliance Virtualization Platform host.                               |
| <b>Platform FQDN</b>                                         | The FQDN of the Appliance Virtualization Platform host.                                     |
| <b>Certificate</b>                                           | The option to select the signed certificate for the Appliance Virtualization Platform host. |
| <b>I agree to accept to add the same certificate in SDM.</b> | The option to accept the certificate in Solution Deployment Manager.                        |

| Button                      | Description                                                                                                                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View/Generate CSR</b>    | Displays the View/Generate CSR dialog box to generate CSR.                                                                                                                                    |
| <b>Download CSR</b>         | Downloads CSR for the selected host.                                                                                                                                                          |
| <b>Browse</b>               | Displays the dialog box where you can choose the signed certificate file. The accepted certificate file formats are: <ul style="list-style-type: none"> <li>• .crt</li> <li>• .pki</li> </ul> |
| <b>Retrieve Certificate</b> | Displays the Certificate dialog box with the details of the uploaded signed certificate.                                                                                                      |
| <b>Push Certificate</b>     | Pushes the uploaded signed certificate to the selected Appliance Virtualization Platform host.                                                                                                |
| <b>Cancel</b>               | Cancels the push operation.                                                                                                                                                                   |

## Create or edit CSR field descriptions

| Name                     | Description                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Organization</b>      | The organization name of the CSR.                                                                                                   |
| <b>Organization Unit</b> | The organization unit of the CSR.                                                                                                   |
| <b>Locality</b>          | The locality of the organization associated with the CSR.                                                                           |
| <b>State</b>             | The state of the organization associate with the CSR.                                                                               |
| <b>Country</b>           | The country of the organization associate with the CSR.<br>In the Edit mode, you can specify only two letters for the country name. |
| <b>Email</b>             | The email address associate with the CSR.                                                                                           |

| Button                 | Description                                                   |
|------------------------|---------------------------------------------------------------|
| <b>Create/Edit CSR</b> | Saves or edits the information entered associated to the CSR. |
| <b>Cancel</b>          | Cancels the add or edit operation of the CSR.                 |

## Virtual Machine snapshot on Appliance Virtualization Platform

When you apply an update by using Solution Deployment Manager, snapshots are left on Appliance Virtualization Platform. If a snapshot is left on Appliance Virtualization Platform, it is detrimental to system performance and over time can utilize all the available disk space. Therefore, ensure that snapshots are not left on Appliance Virtualization Platform for an extended period of time and are removed on a timely manner.

You can review and delete Virtual Machine snapshots from Appliance Virtualization Platform by using Solution Deployment Manager Snapshot Manager.

### Related links

[Deleting the virtual machine snapshot by using Solution Deployment Manager](#) on page 1342  
[Snapshot Manager field descriptions](#) on page 1343

## Deleting the virtual machine snapshot by using Solution Deployment Manager

### About this task

Use this procedure to delete the virtual machine snapshots that reside on the Appliance Virtualization Platform host by using Solution Deployment Manager.

### Procedure

- To access Solution Deployment Manager, do one of the following:
  - On the System Manager web console, click **Services** > **Solution Deployment Manager**.
  - On the desktop, click the Solution Deployment Manager icon ().
- In **Application Management Tree**, select a location.
- On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select the Appliance Virtualization Platform host.



4. Click **More Actions > Snapshot Manager**.

The system displays the Snapshot Manager dialog box.

5. Select one or more snapshots, and click **Delete**.

You must review all listed snapshots and remove snapshots that are more than 24 hours old.

The system deletes the selected snapshots.

### Related links

[Virtual Machine snapshot on Appliance Virtualization Platform](#) on page 1342

### Snapshot Manager field descriptions

| Name                 | Description                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------|
| VM ID                | The ID of the virtual machine.                                                                     |
| Snapshot Age         | The duration of snapshot creation.<br>For example: 75 days 19 hours                                |
| VM Name              | The name of the virtual machine.                                                                   |
| Snapshot Name        | The name of the snapshot.                                                                          |
| Snapshot Description | The description of the snapshot.                                                                   |
| SDM Snapshot         | The snapshot taken from Solution Deployment Manager.<br>The options are <b>Yes</b> and <b>No</b> . |

| Button | Description                                 |
|--------|---------------------------------------------|
| Cancel | Exits from the Snapshot Manager dialog box. |
| Delete | Deletes the selected snapshot.              |

### Related links

[Virtual Machine snapshot on Appliance Virtualization Platform](#) on page 1342

### Add and Edit platform field descriptions

| Name                | Description                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location            | The location where the platform is available. The field is read only.                                                                                                                                                                                                                                                                               |
| Platform Name       | The platform name of OS, Appliance Virtualization Platform or ESXi.                                                                                                                                                                                                                                                                                 |
| Platform FQDN or IP | The IP address or FQDN of OS, Appliance Virtualization Platform or ESXi.                                                                                                                                                                                                                                                                            |
| User Name           | The user name to log in to OS, Appliance Virtualization Platform or ESXi.<br><br><div>  <b>Note:</b><br/>           For Appliance Virtualization Platform, provide the admin credentials that you configured while generating the Kickstart file.         </div> |
| Password            | The password to log in to OS, Appliance Virtualization Platform or ESXi.                                                                                                                                                                                                                                                                            |

| Button | Description                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------|
| Save   | Saves the host information and returns to the Platforms for Selected Location <location name> section. |

## Change Network Parameters field descriptions

### Network Parameters

| Name                 | Description                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                 | The name of the Appliance Virtualization Platform host. The field is display-only.                                                                                                    |
| IPv4                 | The IPv4 address of the Appliance Virtualization Platform host.                                                                                                                       |
| Subnet Mask          | The subnet mask of the Appliance Virtualization Platform host.                                                                                                                        |
| IPv6                 | The IPv6 address of the Appliance Virtualization Platform host (if any).                                                                                                              |
| Host Name            | The host name of the Appliance Virtualization Platform host                                                                                                                           |
| Domain Name          | The domain name of the Appliance Virtualization Platform host                                                                                                                         |
| Preferred DNS Server | The preferred DNS server                                                                                                                                                              |
| Alternate DNS Server | The alternate DNS server                                                                                                                                                              |
| NTP Server1 IP/FQDN  | The NTP Server1 IP address of the Appliance Virtualization Platform host.                                                                                                             |
| NTP Server2 IP/FQDN  | The NTP Server2 IP address of the Appliance Virtualization Platform host.                                                                                                             |
| IPv4 Gateway         | The gateway IPv4 address.<br>The field is available only when you click <b>Change IPv4 Gateway</b> .                                                                                  |
| IPv6 Default Gateway | The default gateway IPv6 address (if any).<br>The field is available only when IPv6 has been configured for the system.<br>The user, also needs to click <b>Change IPv6 Gateway</b> . |

| Button                             | Description                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change IPv4 Gateway                | Makes the <b>IPv4 Gateway</b> field available, and displays <b>Save IPv4 Gateway</b> and <b>Cancel IPv4 Gateway Change</b> buttons.                         |
| Change IPv6 Gateway                | Makes the <b>IPv6 Default Gateway</b> field available, and displays <b>Save IPv6 Default Gateway</b> and <b>Cancel IPv6 Default Gateway Change</b> buttons. |
| Save IPv4 Gateway                  | Saves the gateway IPv4 address value that you provide.                                                                                                      |
| Cancel IPv4 Gateway Change         | Cancels the changes made to the IPv4 gateway.                                                                                                               |
| Save IPv6 Default Gateway          | Saves the default IPv6 gateway address value that you provide.                                                                                              |
| Cancel IPv6 Default Gateway Change | Cancels the changes made to the IPv6 default gateway.                                                                                                       |

| Button | Description                                            |
|--------|--------------------------------------------------------|
| Save   | Saves the changes that you made to network parameters. |

## Host Network / IP Settings field descriptions

### Standard Switches

vSwitch <n> displays the PortGroups and NICs sections.

### PortGroups

| Name                                                                                                     | Description                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  or <b>VLAN ID</b> link | Displays the Port Group Properties page where you configure VLAN ID.                                                                                                       |
| <b>VLAN ID</b>                                                                                           | Displays the VLAN ID. The options are: <ul style="list-style-type: none"> <li>• <b>None (0)</b></li> <li>• <b>1 to 4093</b></li> </ul> The field displays only unused IDs. |

| Button        | Description                          |
|---------------|--------------------------------------|
| <b>OK</b>     | Saves the changes.                   |
| <b>Cancel</b> | Returns to the <b>Platforms</b> tab. |

### NICs

| Name               | Description                                              |
|--------------------|----------------------------------------------------------|
| <b>NIC Name</b>    | Displays the name of the NIC.<br>For example, vmnic0.    |
| <b>Speed</b>       | Displays the speed of the NIC.<br>For example, 100,Full. |
| <b>Link Status</b> | Displays the status of the NIC.                          |

| Button                  | Description                                                           |
|-------------------------|-----------------------------------------------------------------------|
| <b>Change NIC speed</b> | Displays the vmnic<n> dialog box.                                     |
| <b>NIC team/unteam</b>  | Displays the Out of Band Management Properties vSwitch<n> dialog box. |

### NIC speed

| Name                            | Description                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configured speed, Duplex</b> | Displays the NIC speed. The options are: <ul style="list-style-type: none"> <li>• <b>Autonegotiate</b></li> <li>• <b>10,Half</b></li> <li>• <b>10,Full</b></li> <li>• <b>100,Half</b></li> <li>• <b>100,Full</b></li> <li>• <b>1000,Full</b></li> </ul> |

| Button | Description        |
|--------|--------------------|
| OK     | Saves the changes. |

### NIC teaming

| Button    | Description                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------|
| Move Up   | Moves the VMNIC from unused adapters to standby or active adapters or from standby to active adapter. |
| Move Down | Moves the VMNIC from active to standby adapter or from standby to unused adapter.                     |
| Refresh   | Refreshes the page.                                                                                   |
| OK        | Saves the changes.                                                                                    |

### Advanced Configuration

Displays the Unused PortGroups section.

| Name           | Description                  |
|----------------|------------------------------|
| Port Group     | Displays the port group.     |
| Virtual Switch | Displays the virtual switch. |

| Button | Description                          |
|--------|--------------------------------------|
| Delete | Deletes the selected port group.     |
| Cancel | Returns to the <b>Platforms</b> tab. |

### Change Password field descriptions

| Name                 | Description                                               |
|----------------------|-----------------------------------------------------------|
| Current Password     | The password for the user you input when adding the host. |
| New Password         | The new password                                          |
| Confirm New Password | The new password                                          |

| Button          | Description             |
|-----------------|-------------------------|
| Change Password | Saves the new password. |

## Update Host field descriptions

| Name                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Patch location</b>              | <p>The location where the Appliance Virtualization Platform patch is available. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Select Patch from Local SMGR:</b> To use the Appliance Virtualization Platform patch that is available on the local System Manager.</li> <li>• <b>Select Patch from software library:</b> To use the Appliance Virtualization Platform patch that is available in the software library.</li> </ul> |
| <b>Ignore Signature Validation</b> | <p>Ignores the signature validation for the patch.</p> <p> <b>Note:</b></p> <p>If the Appliance Virtualization Platform patch is unsigned, you must select the <b>Ignore signature validation</b> check box.</p>                                                                                                                                                   |
| <b>Select patch file</b>           | The absolute path to the Appliance Virtualization Platform patch file.                                                                                                                                                                                                                                                                                                                                                                              |

| Button             | Description                                                       |
|--------------------|-------------------------------------------------------------------|
| <b>Update Host</b> | Installs the patch on the Appliance Virtualization Platform host. |

## Certificate validation

### Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can establish a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x and later applications. This provides secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts or vCenter.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third-party certificates.

You can check the following with certificate-based TLS sessions:

- Certificate valid dates
- Origin of Certificate Authority
- Chain of Trust
- CRL or OCSP state
- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate SAN or the certificate Common Name and the certificate must be in date.
- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.
- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

For more information about updating the certificate, see “Updating the certificate on the ESXi host from VMware”.

 **Note:**

Solution Deployment Manager:

- Validates certificate of vCenter
- Validates the certificates when a virtual machine is deployed or upgraded on vCenter managed hosts

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can open the web page of the host. The system displays the existing certificate and you can match the details.

## Generating and accepting the Appliance Virtualization Platform host certificates

### About this task

With Solution Deployment Manager, you can generate certificates only for Appliance Virtualization Platform hosts.

If the certificate is invalid:

- Get a correct certificate for the host and add the certificate.
- Regenerate a self-signed certificate on the host.

### Before you begin

Get permissions to add a host to generate certificates.

## Procedure

1. To access Solution Deployment Manager, do one of the following:
  - On the System Manager web console, click **Services > Solution Deployment Manager**.
  - On the desktop, click the Solution Deployment Manager icon ().
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions > Generate/Accept Certificate**.
5. To accept the certificate, in the Certificate dialog box, click **Generate Certificate**, and do the following:
  - a. In the Generate Certificate dialog box, in the **Validity in Days** field, type the validity of the certificate in days.
  - b. Click **Generate Certificate**.  
The system displays the message: Certificate is generated.
  - c. Click **Ok**.
6. To accept the certificate, click **Accept Certificate**.
7. To view the certificate validity status, click the **View link** in the **Platform Certificate Status** column.

Appliance Virtualization Platform places an IP address and FQDN in generated certificates. Therefore, from Solution Deployment Manager, you can connect to Appliance Virtualization Platform hosts through IP address or FQDN.

In the Platforms for Selected Location <location name> section, the **Platform Certificate Status** column must display a check mark .

### **Note:**

An alarm is generated everyday if the certificate expiry is below 60 days. This alarm can be cleared by installing a new identity certificate, which has the validity more than 60 days.

## Generating and updating the certificate on the ESXi host from VMware

### About this task

Generate new certificates only if you change the host name or accidentally delete the certificate. Under certain circumstances, you must force the host to generate new certificates.

To receive the full benefit of certificate checking, particularly if you want to use encrypted remote connections externally, do not use a self-signed certificate. Instead, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority.

## Procedure

To generate and update ESXi host and vCenter certificates, see the VMware documentation.

## Next steps

### \* Note:

The host certificate must match the fully qualified domain name of the host.

VMware places only FQDN in certificates that are generated on the host. Therefore, use a fully qualified domain name to connect to ESXi hosts and vCenter from Solution Deployment Manager.

The connection from Solution Deployment Manager 7.1 and later to a vCenter or ESXi host by using an IP address fails because the IP address is absent in the certificate and the connection is not sufficiently secure.

## Managing certificates for existing hosts

### About this task

By default, the certificate status of the host or vCenter that is migrated from earlier release is invalid. To perform any operation on the host from Solution Deployment Manager, you require a valid certificate. Therefore, you must get the valid certificate and accept the certificate.

### Before you begin

Gain permissions to add a host to generate certificates.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. For the ESXi host, do one of the following:
  - If the certificate is valid, on the Certificate dialog box, click **More Actions > Generate/ Accept Certificate**, and click **Accept Certificate**.
  - If the certificate is invalid, log in to the ESXi host, validate the certificate, and then from Solution Deployment Manager, accept the certificate.

For more information, see “Generating and updating the certificate on the ESXi host from VMware”.



## Managing the application

### Deploying AVP Utilities

#### About this task

Use this procedure to deploy AVP Utilities on Appliance Virtualization Platform.

To deploy AVP Utilities, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client, when System Manager is unavailable.

#### Before you begin

- Add a location.

See “Adding a location” in *Administering Avaya Aura® System Manager*.

- Add Appliance Virtualization Platform.

See “Adding an Appliance Virtualization Platform or ESXi host” in *Administering Avaya Aura® System Manager*.

- Download the AVP Utilities OVA file.

#### Procedure

1. To access Solution Deployment Manager, do one of the following:
  - On the System Manager web console, click **Services > Solution Deployment Manager**.
  - On the desktop, click the Solution Deployment Manager icon .
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

The system displays the Applications Deployment section.

4. In the Select Location and Platform section, do the following:
  - a. In **Select Location**, select a location.
  - b. In **Select Platform**, select a platform.

The system displays the host name in the **Platform FQDN** field.

5. In **Data Store**, select a data store, if not displayed upon host selection.

The page displays the capacity details.

6. Click **Next**.

7. To get the OVA file, select the **OVA** tab, and click one of the following:

- **URL**, in **OVA File**, type the absolute path to the application OVA file, and click **Submit**.
- **S/W Library**, in **File Name**, select the application OVA file.

- **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.

If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the message: `Invalid file content. Avaya Certificate not found or invalid.`

8. Click **Next**.

In the Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.

9. In the Network Parameters section, ensure that the following fields are preconfigured:

- **Public**
- **Services**
- **Out of Band Management**.

For more information, see “Application Deployment field descriptions”.

10. In the Configuration Parameters section, complete the fields.

For more information about Configuration Parameters, see “Network Parameters and Configuration Parameters field descriptions”.

11. Click **Deploy**.

12. Click **Accept the license terms**.

In the Platforms for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

The system displays the virtual machine on the Applications for Selected Location <location name> page.

13. To view the details, click the **Status Details** link.

### Next steps

1. To activate the serviceability agent registration, reboot the AVP Utilities virtual machine.
2. Deploy all other Avaya Aura® applications at a time.

### Related links

[Application Deployment field descriptions](#) on page 1364

## Deploying an OVA file for an Avaya Aura® application

### About this task

Use the procedure to deploy an OVA file for an Avaya Aura® application on the virtual machine.

To deploy an Avaya Aura® application, you can use Solution Deployment Manager from System Manager or the Solution Deployment Manager client if System Manager is unavailable.

Deploy AVP Utilities first, and then deploy all other applications one at a time.

## Before you begin

- Add a location.
- Add Appliance Virtualization Platform or an ESXi host to the location.
- Ensure that the certificate is valid on the Appliance Virtualization Platform host or vCenter managed hosts.
- Download the required OVA file to System Manager.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a platform.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, click **New**.

The system displays the Applications Deployment section.

4. In the Select Location and Platform section, do the following:
  - a. In **Select Location**, select a location.
  - b. In **Select Platform**, select a platform.

The system displays the host name in the **Platform FQDN** field.

5. In **Data Store**, select a data store, if not displayed upon host selection.

The page displays the capacity details.

6. Click **Next**.

7. To get the OVA file, select the **OVA** tab, and click one of the following:

- **URL**, in **OVA File**, type the absolute path to the application OVA file, and click **Submit**.
- **S/W Library**, in **File Name**, select the application OVA file.
- **Browse**, select the required application OVA file from a location on the computer, and click **Submit File**.

If the OVA file does not contain a valid Avaya certificate, then the system does not parse the OVA and displays the message: Invalid file content. Avaya Certificate not found or invalid.

8. In **Flexi Footprint**, select the footprint size that the application supports.
9. **(Optional)** To install the patch file for the Avaya Aura® application, click **Service or Feature Pack**, and enter the appropriate parameters.
  - **URL**, and type the absolute path of the same local windows computer or the http URL accessible from the same local windows computer of the latest service or feature pack.
  - **S/W Library**, and select the latest service or feature pack from the drop-down list.
  - **Browse**, and select the latest service or feature pack from your local computer, and click **Submit File**.

You can install the patch file for the Avaya Aura® application now or after completing the Avaya Aura® application OVA deployment.

10. Click **Next**.

In Configuration Parameters and Network Parameters sections, the system displays the fields that are specific to the application that you deploy.

11. In the Network Parameters section, ensure that the following fields are preconfigured:

- **Public**
- **Services:** Only for AVP Utilities.
- **Duplicate Link:** Only for duplex Communication Manager.
- **Private:** Only for Application Enablement Services.
- **Out of Band Management.**

For more information, see “Application Deployment field descriptions”.

12. In the Configuration Parameters section, complete the fields.

For each application that you deploy, fill the appropriate fields. For more information, see “Application Deployment field descriptions”.

13. Click **Deploy**.

14. Click **Accept the license terms**.

In the Platforms for Selected Location <location name> section, the system displays the deployment status in the **Current Action Status** column.

The system displays the virtual machine on the Applications for Selected Location <location name> page.

15. To view details, click **Status Details**.

## Next steps

Perform the following for Communication Manager:

1. From the Manage Elements link on System Manager, update the credentials corresponding to the element that you added.
2. Before the synchronization and after deployment, add an SMNP profile on Communication Manager.

 **Note:**

If you fail to update the password, the synchronization operation fails.

## Related links

[Installing software patches by using Solution Deployment Manager](#) on page 1357

[Application Deployment field descriptions](#) on page 1364

## Refreshing elements

### Before you begin

- On the User Settings page, configure the user settings.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
  - a. Select one or more devices.
  - b. Click **Pre-upgrade Actions > Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
  - **Run Immediately**: To perform the job.
  - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

The **Last Action Status** column displays  and the **Current Version** column displays the current version of the element.

## Analyzing software

### About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

### Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
  - a. Select a device that you want to analyze.
  - b. Click **Pre-upgrade Actions > Analyze**.
4. On the Job Schedule page, click one of the following:
  - **Run Immediately**: To perform the job.

- **Schedule later:** To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
  6. Click **Schedule**.

The **Last Action Status** column displays a , the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

## Re-establishing trust for Solution Deployment Manager elements

### About this task

Use this procedure to re-establish trust with an application.

### Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

### Procedure

1. To access Solution Deployment Manager, do one of the following:
  - On the System Manager web console, click **Services > Solution Deployment Manager**.
  - On the desktop, click the Solution Deployment Manager icon ().
2. Click **Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the **Applications** tab, in the Applications for Selected Location <location name> area, select an application.
5. Click **More Actions > Re-establish connection**.
6. Select the release version of the product deployed on the application.

The options are:

  - **6.3 and below**
  - **7.0**
  - **7.1 and above**
  - **others**
7. In **User Name**, type the user name of the application.
8. In **Password**, type the password of the application.
9. Click **Reestablish Connection**.

## Installing software patches by using Solution Deployment Manager

### About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

#### \* Note:

When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions > Installed Patches** on the Upgrade Management page, then perform the following:

1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
2. Refresh the element.

### Before you begin

- Perform refresh and analyze operations.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions > Re-establish Connection**.
  3. Click **Refresh VM**.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions > Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

#### \* Note:

If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.

9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.

11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

If the field displays , review the information on the Edit Upgrade Configuration page.

12. Click **Upgrade**.

13. On the Job Schedule page, click one of the following:

- **Run Immediately**: To perform the job.
- **Schedule later**: To perform the job at a scheduled time.

14. Click **Schedule**.

On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .

15. To view the update status, click .

The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

When the update is complete, the **Update status** and **Last Action Status** fields displays .

16. Click **Upgrade Actions > Installed Patches**.

17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

The page displays all software patches that you can commit.

You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

You can schedule to commit the patch at a later time by using the **Schedule later** option.

19. Click **Schedule**.

The Upgrade Management page displays the last action as **Commit**.

20. Ensure that **Update status** and **Last Action Status** fields display .

 **Note:**

If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

## Editing an application

### Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.



- When you change the IP address or FQDN:
  - AVP Utilities must be available and must be discovered.
  - If AVP Utilities is discovered, the system must display AVP Utilities in the **App Name** column. If the application name in **App Name** is empty, click **More Actions > Re-establish connection** to establish trust between the application and System Manager.

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, select an application, and click **Edit**.

The system displays the Edit App section.

4. To update the IP address and FQDN of the application in the local Solution Deployment Manager inventory, perform the following:
  - a. Click **More Actions > Re-establish connection**.

 **Note:**

To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

- b. Click **More Actions > Refresh App**.

 **Note:**

To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

- c. Click **Update IP/FQDN in Local Inventory**.
- d. Click **Update App IP/FQDN**.
- e. Provide the IP address and FQDN of the application.

**Update IP/FQDN in Local Inventory** updates the IP address or FQDN of the application only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the **Platforms** tab to update the IP address or FQDN of the host.

5. Click **Save**.

## Deleting an application

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.

3. On the **Applications** tab, select one or more application.
4. On the Delete page, click **Delete**, and click **Yes** to confirm the deletion.

The system turns off the applications, and deletes the selected applications from the platform.

## Updating Services Port Static Routing on an Avaya Aura® application

### About this task

You might have to change the static routing if the Avaya Aura® application that is running on the Appliance Virtualization Platform host is:

- Deployed by using the vSphere Web Client and does not have the route.
- Non-operational or unreachable when you start the Avaya Aura® application update.

### Before you begin

- Update network parameters of AVP Utilities if applicable.
- Ensure that the Avaya Aura® application resides on the same subnet as AVP Utilities.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the Applications tab, in the Applications for Selected Location <location name> section, select an Avaya Aura® application.
3. Click **More Actions > Update Static Routing**.

The VM Update Static Routing page displays the details of Avaya Aura® application and AVP Utilities. The fields are read-only.

4. Click **Update**.
5. On the Success dialog box, click **OK**.

The system updates the Avaya Aura® application with the new IP address of AVP Utilities for Services Port static routing.

### Related links

[Update Static Routing field descriptions](#) on page 1373

## Starting an application from Solution Deployment Manager

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the **Application Management Tree**, select a platform to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to start.
4. Click **Start**.

In **Application State**, the system displays *Started*.

## Stopping an application from Solution Deployment Manager

### About this task

System Manager is operational and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the **Application Management Tree**, select a ESXi or vCenter host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to stop.
4. Click **Stop**.

In **Application State**, the system displays *Stopped*.

## Restarting an application from Solution Deployment Manager

### Before you begin

- System Manager is operational, and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.
- Applications must be in the running state.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the application management tree, select a host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to restart.
4. Click **Restart**.

In **Application State**, the system displays *Stopped* and then *Started*.

## VM Console overview

From Release 8.1.1, you can open the VM console in a new browser window or on a new browser tab.

To open and manage the application through the console, ensure that the:

- Application must be in running state. The application status must be **Started** for the application on the **Applications** tab in the **Application State** column.
- Application must reside on the Appliance Virtualization Platform host Release 7.1.2 and later.
- Appliance Virtualization Platform host certificate must be added in your browser.

You cannot view the VM Console of the application if the application resides on the customer-provided VMware ESXi host.

## Opening a VM console from Solution Deployment Manager

### About this task

Use the following procedure to open the VM console in a new browser window or on a new browser tab.

### Before you begin

- Add a location.
- Add the Appliance Virtualization Platform host.
- Ensure that the application is hosted on the Appliance Virtualization Platform host.
- Add the Appliance Virtualization Platform host certificate in your browser.

If you do not add the host certificate in your browser, the system displays the following message when you try to open the VM console in a browser:

To open VM Console of an application, add the Platform certificate in the browser. Following is the URL of the platform to accept the certificate: `https://<Host URL where the application resides>:443`

### Procedure

1. To access Solution Deployment Manager, do one of the following:
  - On the System Manager web console, click **Services > Solution Deployment Manager**.
  - On the desktop, click the Solution Deployment Manager icon ().
2. Click **Application Management**.
3. In **Application Management Tree**, select a location.
4. On the **Applications** tab, in the **Applications for Selected Location <location name>** section, select the application.
5. To open the VM console in a new:
  - Browser window, click **VM Console > Open VM Console in New Window**.
  - Tab of the browser, click **VM Console > Open VM Console in New Tab**.

When you open the console for the very first time, if the Appliance Virtualization Platform host certificate is not added in your browser, the system opens the browser instance with the following message:

To open VM Console of an application, add the Platform certificate in the browser. Following is the URL of the platform to accept the certificate: `https://<Host URL where the application resides>:443`

If you open the VM console after accepting the Appliance Virtualization Platform host certificate in the browser, the system opens the VM console without any warning message.

If the browser displays the same error message even after accepting the Appliance Virtualization Platform host certificate, see *Troubleshooting Avaya Aura® System Manager*.

### Next steps

On VM Console, log in to the application and perform the required operations.

### VM Console field descriptions

| Name                   | Description                                                                                                                                                                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Full Screen</b>     | Opens the console in full screen mode.<br>You can press the <b>Esc</b> key to exit from the full screen mode.                                                                                                                                                                                                |
| <b>Send Keys</b>       | These keys are applied to the VM Linux system and not to your local computer from where you are accessing the VM Console.<br>The options are: <ul style="list-style-type: none"> <li>• <b>Send Ctrl+Alt+Del</b></li> <li>• <b>Send Ctrl+c</b></li> <li>• <b>Send Escape</b></li> </ul>                       |
| <b>KeyBoard Layout</b> | Sets the keyboard layout based on the selected language.<br>The options are: <ul style="list-style-type: none"> <li>• English</li> <li>• Japanese</li> <li>• German</li> <li>• Italian</li> <li>• Spanish</li> <li>• Portuguese</li> <li>• French</li> <li>• Swiss-French</li> <li>• Swiss-German</li> </ul> |

### Common causes for application deployment failure

If the application is not reachable from System Manager Solution Deployment Manager or Solution Deployment Manager Client, the OVA deployment fails at the sanity stage, because you might have:

- Provided an IP which is not on the network.
- Provided wrong network values that causes the network configuration for the application to not work properly.
- Chosen a private virtual network.

The following are some examples of wrong network values and configuration that can result in the OVA deployment failure:

- Using an IP which is already there on the network (duplicate IP).
- Using an IP which is not on your network at all.
- Using a DNS value, such as 0.0.0.0.
- Deploying on an isolated network on your VE deployment.

You can check the deployment status in the **Current Action Status** column on the **Applications** tab.

## Application Deployment field descriptions

### Select Location and Platform

| Name                   | Description                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Select Location</b> | The location name.                                                                                              |
| <b>Select Platform</b> | The platform name that you must select.                                                                         |
| <b>Platform FQDN</b>   | The platform FQDN.                                                                                              |
| <b>Data Store</b>      | The data store for the application.<br>The page populates the capacity details in the Capacity Details section. |
| <b>Next</b>            | Displays the OVA/ISO Details section where you provide the details required for OVA or ISO deployment.          |

### Capacity Details

The system displays the CPU and memory details of the AVP or ESXi host. The fields are read-only.

#### **Note:**

If the host is in a cluster, the system does not display the capacity details of CPU and memory. Ensure that the host resource requirements are met before you deploy the virtual machine.

| Name                     | Description              |
|--------------------------|--------------------------|
| <b>Name</b>              | The name                 |
| <b>Full Capacity</b>     | The maximum capacity     |
| <b>Free Capacity</b>     | The available capacity   |
| <b>Reserved Capacity</b> | The reserved capacity    |
| <b>Status</b>            | The configuration status |

### Provide admin and root Credentials

The system displays the Provide admin and root Credentials section for OS.

| Name                 | Description                |
|----------------------|----------------------------|
| Platform IP          | The platform IP.           |
| Platform FQDN        | The platform FQDN          |
| Admin User of OS     | The admin user name of OS. |
| Admin Password of OS | The admin password of OS.  |
| Root User of OS      | The root user of OS.       |

### Deploy OVA using System Manager Solution Deployment Manager

| Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ME Deployment            | <p>The option to perform the Midsize Enterprise deployment.</p> <p>The option to perform the Midsize Enterprise deployment.</p> <p>The option is available only while deploying Communication Manager simplex OVA.</p>                                                                                                                                                                                                                                                                |
| Enable enhanced security | The option to enable JITC mode deployment.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Select Software Library  | The software library where the .ova file is available.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Select OVAs              | <p>The .ova file that you want to deploy.</p> <p> <b>Note:</b></p> <p>System Manager validates any file that you upload during deployment, and accepts only OVA file type. System Manager filters uploaded files based on file extension and mime types or bytes in the file.</p>                                                                                                                    |
| Flexi Footprint          | <p>The footprint size supported for the selected application.</p> <p> <b>Important:</b></p> <ul style="list-style-type: none"> <li>• Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory.</li> <li>• Ensure that the application contains the footprint size values that are supported.</li> </ul> |
| Next                     | Displays the Configuration Parameters tab in the OVA Details screen where you provide the OVA details.                                                                                                                                                                                                                                                                                                                                                                                |

### Deploy OVA using the Solution Deployment Manager client

| Name          | Description                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ME Deployment | <p>The option to perform the Midsize Enterprise deployment.</p> <p>The option to perform the Midsize Enterprise deployment.</p> <p>The option is available only while deploying Communication Manager simplex OVA.</p> |

The system displays the following options for deployment by providing OVA path.

| Name               | Description                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Browse</b>      | The option to enter the full/absolute path of the .ova file to install it as a virtual machine on the system that hosts the Solution Deployment Manager client.                 |
| <b>OVA File</b>    | The absolute path to the .ova file on the system that hosts the Solution Deployment Manager client.<br><br>The field is available only when you click <b>Provide OVA Path</b> . |
| <b>Submit File</b> | Selects the .ova file of System Manager that you want to deploy.                                                                                                                |

With the **S/W Library** option you can select a .ova file that is available in the local software library of windows machine where the Solution Deployment Manager client is installed.

The system displays the following options for deployment using local software library.

| Name             | Description                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>File Name</b> | The file name of the .ova file that is to be installed on the system that hosts the Solution Deployment Manager client.<br><br>The field is available only when you click <b>S/W Library</b> . |

With the **URL** option, you can type the URL of the OVA or ISO file. The system displays the following options.

| Name          | Description                                                                                    |
|---------------|------------------------------------------------------------------------------------------------|
| <b>URL</b>    | The URL of the OVA or ISO file.<br><br>The field is available only when you click <b>URL</b> . |
| <b>Submit</b> | Selects the OVA or ISO file to be deployed that is extracted from the URL.                     |

The system displays the following common fields.

| Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Flexi Footprint</b> | The footprint size supported for the selected application.<br><br>The field is available for all three types of deployment.<br><br> <b>Important:</b><br><br>Ensure that the required memory is available for the footprint sizes that you selected. The upgrade operation might fail due to insufficient memory. |
| <b>Next</b>            | Displays the <b>Configuration Parameters</b> tab in the OVA Details section where you provide the OVA details.                                                                                                                                                                                                                                                                                       |

## Configuration Parameters

The system populates most of the fields depending on the OVA file.



**\* Note:**

For configuration parameter fields, for Communication Manager Messaging and AVP Utilities, see [Configuration and Network Parameters field descriptions](#) on page 1369.

| Name                    | Description                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------|
| <b>Application Name</b> | The name of the application.                                                                     |
| <b>Product</b>          | The name of the Avaya Aura® application that is being deployed.<br>The field is read-only.       |
| <b>Version</b>          | Release number of the Avaya Aura® application that is being deployed.<br>The field is read-only. |

### Communication Manager Configuration Parameters

| Name                                              | Description                                                                                                                                                                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CM IPv4 Address</b>                            | The IPv4 address of the Communication Manager virtual machine.                                                                                                                                                                |
| <b>CM IPv4 Netmask</b>                            | The IPv4 network mask of the Communication Manager virtual machine.                                                                                                                                                           |
| <b>CM IPv4 Gateway</b>                            | The IPv4 default gateway of the Communication Manager virtual machine.                                                                                                                                                        |
| <b>CM IPv6 Address</b>                            | The IPv6 address of the Communication Manager virtual machine.<br>The field is optional.                                                                                                                                      |
| <b>CM IPv6 Network Prefix</b>                     | The IPv6 network prefix of the Communication Manager virtual machine.<br>The field is optional.                                                                                                                               |
| <b>CM IPv6 Gateway</b>                            | The IPv6 gateway of the Communication Manager virtual machine.<br>The field is optional.                                                                                                                                      |
| <b>Out of Band Management IPv4 Address</b>        | The IPv4 address of the Communication Manager virtual machine for out of band management.<br>The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network. |
| <b>Out of Band Management IPv4 Netmask</b>        | The IPv4 subnet mask of the Communication Manager virtual machine for out of band management.                                                                                                                                 |
| <b>Out of Band Management IPv6 Address</b>        | The IPv6 address of the Communication Manager virtual machine for out of band management.<br>The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network. |
| <b>Out of Band Management IPv6 Network Prefix</b> | The IPv6 subnet mask of the Communication Manager virtual machine for out of band management.                                                                                                                                 |
| <b>CM Hostname</b>                                | The hostname of the Communication Manager virtual machine.                                                                                                                                                                    |

*Table continues...*

| Name                                             | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NTP Server(s)</b>                             | The IP address or FQDN of the NTP server.<br>Separate the IP addresses with commas (,).<br>You can type up to three NTP servers.                                                                                                                                                                                                                                                                     |
| <b>DNS Server(s)</b>                             | The DNS IP address of the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                     |
| <b>Search Domain List</b>                        | The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).                                                                                                                                                                                                                                                                                          |
| <b>WebLM Server IPv4 Address</b>                 | The IPv4 address of WebLM. The field is mandatory.                                                                                                                                                                                                                                                                                                                                                   |
| <b>EASG User Access</b>                          | Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks.<br><br>The options are:<br><ul style="list-style-type: none"> <li>• 1: To enable EASG.</li> <li>• 2: To disable EASG.</li> </ul> Avaya recommends to enable EASG.<br><br>You can also enable EASG after deploying or upgrading the application by using the command: <b>EASGManage --enableEASG</b> . |
| <b>CM Privileged Administrator User Login</b>    | The login name for the privileged administrator. You can change the value at any point of time. The field is mandatory.                                                                                                                                                                                                                                                                              |
| <b>CM Privileged Administrator User Password</b> | The password for the privileged administrator. You can change the value at any point of time. The field is mandatory.                                                                                                                                                                                                                                                                                |
| <b>Confirm Password</b>                          | The password required to be confirmed. The field is mandatory.                                                                                                                                                                                                                                                                                                                                       |

## Customer Root Account

### \* Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

| Name                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Customer Root Account for this Application</b> | Enables or disables the customer root account for the application.<br><br>Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click <b>Accept</b> .<br><br>When you accept the root access statement, the system displays the <b>Customer Root Password</b> and <b>Re-enter Customer Root Password</b> fields. |
| <b>Customer Root Password</b>                            | The root password for the application                                                                                                                                                                                                                                                                                                       |

*Table continues...*

| Name                                   | Description                           |
|----------------------------------------|---------------------------------------|
| <b>Re-enter Customer Root Password</b> | The root password for the application |

## Network Parameters

| Name                          | Description                                                                                                                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Public</b>                 | The port number that is mapped to public port group.<br><br>You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.                        |
| <b>Services</b>               | The port number that is mapped to the services port group when AVP Utilities is deployed in the solution.<br><br>AVP Utilities provides routing from the services port to the virtual machines and additional functions, such as alarm conversion. |
| <b>Duplication Link</b>       | The connection for server duplication.<br><br>The field is available only when you deploy duplex Communication Manager.                                                                                                                            |
| <b>Private</b>                | The field is available only when you deploy Application Enablement Services.                                                                                                                                                                       |
| <b>Create Port Group</b>      | The field to create new port group for interface.                                                                                                                                                                                                  |
| <b>Out of Band Management</b> | The port number that is mapped to the out of band management port group.                                                                                                                                                                           |

| Button        | Description                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------|
| <b>Deploy</b> | Displays the EULA acceptance screen where you must click <b>Accept</b> to start the deployment process. |

## Related links

[Configuration and Network Parameters field descriptions](#) on page 1369

## Configuration and Network Parameters field descriptions

**Table 9: Configuration Parameters for Communication Manager Messaging deployment**

| Name                          | Description                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Messaging IPv4 address</b> | The IP address of the Communication Manager Messaging virtual machine.                               |
| <b>Messaging IPv4 Netmask</b> | The network mask of the Communication Manager Messaging virtual machine.                             |
| <b>Messaging IPv4 Gateway</b> | The default gateway of the Communication Manager Messaging virtual machine. For example, 172.16.1.1. |

*Table continues...*

| Name                                                    | Description                                                                                                                                                                                                                                |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Out of Band Management IPv4 Address</b>              | The IP address of the Communication Manager Messaging virtual machine for out of band management.<br><br>The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network. |
| <b>Out of Band Management IPv4 Netmask</b>              | The subnetwork mask of the Communication Manager Messaging virtual machine for out of band management.                                                                                                                                     |
| <b>Messaging Hostname</b>                               | The hostname of the Communication Manager Messaging virtual machine.                                                                                                                                                                       |
| <b>NTP Servers</b>                                      | The IP address or FQDN of the NTP server.<br><br>Separate the IP addresses with commas (,). The field is optional.                                                                                                                         |
| <b>DNS Server(s)</b>                                    | The DNS IP address of the Communication Manager Messaging virtual machine. Separate the IP addresses with commas(,). The field is optional.                                                                                                |
| <b>Search Domain List</b>                               | The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).                                                                                                                                |
| <b>WebLM Server IPv4 Address</b>                        | The IP address of WebLM. The field is mandatory.                                                                                                                                                                                           |
| <b>Messaging Privileged Administrator User Login</b>    | The login name for the privileged administrator.<br><br>You can change the value at any point of time.                                                                                                                                     |
| <b>Messaging Privileged Administrator User Password</b> | The password for the privileged administrator.<br><br>You can change the value at any point of time.                                                                                                                                       |
| <b>Confirm Password</b>                                 | The password required to be confirmed.                                                                                                                                                                                                     |

### Configuration and Network Parameters for AVP Utilities deployment

| Name                     | Description                                                                                                                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Networking Properties    |                                                                                                                                                                                                                                                                                                                                  |
| <b>Hostname</b>          | Linux hostname or fully qualified domain name for AVP Utilities virtual machine.<br><br><div>  <b>Note:</b> </div> <p>The host name is regardless of the interface that is used to access. The Public interface is the default interface.</p> |
| <b>Public IP address</b> | The IP address for this interface.<br><br>Required field unless you use DHCP.                                                                                                                                                                                                                                                    |
| <b>Public Netmask</b>    | The netmask for this interface.<br><br>Required field unless you use DHCP.                                                                                                                                                                                                                                                       |

*Table continues...*

| Name                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Public Default Gateway</b>                                         | <p>The IP address of the default gateway.</p> <p>Required field unless you use DHCP.</p> <p> <b>Note:</b></p> <p>The default gateway should be configured for the Public network. You can use the <code>ovf_set_static</code> command to allow a static route to be assigned to the OOBM network, enabling OOBM network to reach a second subnet.</p> |
| <b>Public IPv6 address</b>                                            | <p>The IP address for this interface.</p> <p>Required field unless you use DHCP.</p>                                                                                                                                                                                                                                                                                                                                                   |
| <b>Public IPv6 Prefix</b>                                             | <p>The netmask for this interface.</p> <p>Required field unless you use DHCP.</p>                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default IPv6 Gateway</b>                                           | <p>The IP address of the default gateway.</p> <p>Required field unless you use DHCP.</p>                                                                                                                                                                                                                                                                                                                                               |
| <b>Out of Band Management IP Address</b>                              | The IP address for this interface.                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Out of Band Management Netmask</b>                                 | The netmask for this interface.                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Out of Band Management IPv6 Address</b>                            | The IPv6 address for this interface. This field is optional.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Out of Band Management IPv6 Prefix</b>                             | The IPv6 prefix for this interface. This field is optional.                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Network Time Protocol IP</b>                                       | IP address of a server running Network Time Protocol that Communication Manager can use for time synchronization.                                                                                                                                                                                                                                                                                                                      |
| <b>Timezone setting</b>                                               | The selected timezone setting for the AVP Utilities virtual machine.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>DNS</b>                                                            | <p>The IP address of domain name servers for the AVP Utilities virtual machine. Separate each IP address by a comma.</p> <p>Required field unless you use DHCP.</p> <p>You can specify up to three DNS Servers.</p>                                                                                                                                                                                                                    |
| <b>Primary System Manager IP address for application registration</b> | The IP address of System Manager that is required for application registration.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Enrollment Password</b>                                            | The enrollment password.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Confirm Password</b>                                               | The confirmation password.                                                                                                                                                                                                                                                                                                                                                                                                             |
| Application Properties                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AVP Utilities Mode</b>          | <p>The mode in which you want to deploy AVP Utilities. You can set the mode during the deployment only. You cannot change the mode after the virtual machine is deployed. The options are:</p> <ul style="list-style-type: none"> <li>• <b>standard_mode</b>: AVP Utilities and services port enabled. The default mode for Appliance Virtualization Platform.</li> <li>• <b>hardened_mode</b>: Sets up the system for commercial hardening.</li> <li>• <b>hardened_mode (dod)</b>: Sets up the system for military hardening.</li> </ul>      |
| <b>Admin User Password</b>         | The admin user password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Confirm Password</b>            | The confirmation password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Out of Band Management Mode</b> | <p>The Out of Band Management mode in which you want to deploy. The options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>OOBM_Enabled</b>: To enable Out of Band Management.</li> <li>• <b>OOBM_Disabled</b>: To disable Out of Band Management.</li> </ul> <p> <b>Note:</b></p> <p><b>OOBM_Disabled</b> is the default setting. If the mode is set to <b>OOBM_Disabled</b>, then you do not need to configure Out of Band Management.</p> |

## Enhanced Access Security Gateway (EASG) - EASG User Access

| Name                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG</b> | <p>Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• 1: To enable EASG.</li> <li>• 2: To disable EASG.</li> </ul> <p>Avaya recommends to enable EASG.</p> <p>You can also enable EASG after deploying or upgrading the application by using the command: <b>EASGManage --enableEASG</b>.</p> |

## Customer Root Account

### **Note:**

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

| Name                                                     | Description                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Customer Root Account for this Application</b> | Enables or disables the customer root account for the application.<br>Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click <b>Accept</b> .<br><br>When you accept the root access statement, the system displays the <b>Customer Root Password</b> and <b>Re-enter Customer Root Password</b> fields. |
| <b>Customer Root Password</b>                            | The root password for the application                                                                                                                                                                                                                                                                                                   |
| <b>Re-enter Customer Root Password</b>                   | The root password for the application                                                                                                                                                                                                                                                                                                   |

## Update Static Routing field descriptions

| Name                       | Description                                |
|----------------------------|--------------------------------------------|
| <b>VM Name</b>             | The application name.                      |
| <b>VM IP/FQDN</b>          | The IP address or FQDN of the application. |
| <b>Utility Services IP</b> | The IP address of AVP Utilities.           |

| Button        | Description                                |
|---------------|--------------------------------------------|
| <b>Update</b> | Updates the static IP address for routing. |

## Installed Patches field descriptions

| Name                    | Description                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Application Name</b> | The name of the application on which you want to install the patch.                                                                                                    |
| <b>Application IP</b>   | The IP address of the application on which you want to install the patch.                                                                                              |
| <b>Patch Name</b>       | The software patch name that you want to install.                                                                                                                      |
| <b>Patch Type</b>       | The patch type. The options are service pack and software patch.                                                                                                       |
| <b>Patch Version</b>    | The software patch version.                                                                                                                                            |
| <b>Patch State</b>      | The software patch state. The states are: <ul style="list-style-type: none"> <li>• Activated</li> <li>• Deactivated</li> <li>• Removed</li> <li>• Installed</li> </ul> |
| <b>Patch Status</b>     | The software patch status.                                                                                                                                             |

| Button                        | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Action to be performed</b> | The operation that you want to perform on the software patch, service pack, or feature pack that you installed. The options are: <ul style="list-style-type: none"> <li>• <b>All</b>: Displays all the software patches.</li> <li>• <b>Commit</b>: Displays the software patches that you can commit.</li> <li>• <b>Rollback</b>: Displays the software patches that you can rollback.</li> </ul> |
| <b>Get Patch Info</b>         | Displays software patches, service packs, and feature packs that you installed.                                                                                                                                                                                                                                                                                                                   |
| <b>Commit</b>                 | Commits the selected software patch.                                                                                                                                                                                                                                                                                                                                                              |
| <b>Rollback</b>               | Rolls back the selected software patch.                                                                                                                                                                                                                                                                                                                                                           |

## Update App field descriptions

| Name                                   | Description                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VM Name</b>                         | The System Manager virtual machine name.                                                                                                                                                                                                                                                                              |
| <b>VM IP</b>                           | The IP address of System Manager.                                                                                                                                                                                                                                                                                     |
| <b>VM FQDN</b>                         | FQDN of System Manager.                                                                                                                                                                                                                                                                                               |
| <b>Host Name</b>                       | The host name.                                                                                                                                                                                                                                                                                                        |
| <b>Select bin file from Local SMGR</b> | The option to select the software patch or service pack for System Manager.<br><br>The absolute path is the path on the computer on which the Solution Deployment Manager client is running. The patch is uploaded to System Manager.<br><br>This option is available only on the Solution Deployment Manager client. |
| <b>Auto commit the patch</b>           | The option to commit the software patch or service pack automatically.<br><br>If the check box is clear, you must commit the patch from <b>More Actions &gt; Installed Patches</b> .                                                                                                                                  |

| Button         | Description                                                    |
|----------------|----------------------------------------------------------------|
| <b>Install</b> | Installs the software patch or service pack on System Manager. |

## Reestablish Connection field descriptions

| Name                  | Description                                                                                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Version</b> | Select the required version. The options are: <ul style="list-style-type: none"> <li>• <b>6.3 and below</b></li> <li>• <b>7.0</b></li> <li>• <b>7.1 and above</b></li> <li>• <b>others</b></li> </ul> |

*Table continues...*



| Name             | Description                                |
|------------------|--------------------------------------------|
| Application Name | The name of the application.               |
| VM IP/FQDN       | The IP address or FQDN of the application. |
| User Name        | The user name of the application.          |
| Password         | The password of the application.           |

| Button                 | Description                                                        |
|------------------------|--------------------------------------------------------------------|
| Reestablish Connection | Establishes connection between System Manager and the application. |
| Cancel                 | Cancels the changes and returns to the previous page.              |

## Virtual machine report

You can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

The script to generate the virtual machine report is in the `/swlibrary/reports/generate_report.sh` folder.

### Important:

If you run the report generation script when an upgrade is in progress on System Manager, the upgrade might fail.

### generate\_report.sh command

The `generate_report.sh` generates the virtual machine report.

#### Syntax

```
sh ./generate_report.sh [-g] [-u Provide SMGR UI user name] [-p Provide SMGR UI password] [-s] [-a]
```

|                              |                                                        |
|------------------------------|--------------------------------------------------------|
| <b>-g</b>                    | The option to generate the report.                     |
| <b>-u, SMGR UI user name</b> | System Manager Web console user name.                  |
| <b>-p, SMGR UI password</b>  | System Manager Web console password.                   |
| <b>-s</b>                    | The option to view the status of the generated report. |
| <b>-a</b>                    | The option to abort the generated report.              |

## Generating a virtual machine report

### Before you begin

If the application is of prior to Release 7.1, you must establish the trust with all applications before running the Report Generation utility.

## Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -g -u <SMGR UI Username> -p <SMGR UI Password>` command:

For example: `./generate_report.sh -g -u admin -p password`

The system displays the following message: Executing the Report Generation script can cause the failure of upgrade that is running on the System Manager system. Do you still want to continue? [Y/N].

4. To proceed with report generation, type Y, and press Enter.

The system generates the report in the `.csv` format in the `/swlibrary/reports/vm_app_report_DDMMYYYYxxxx.csv` folder.

### \* Note:

If you re-run the report generation script when the report generation process is in progress, the system displays the following message: Report Generation Process is Already Running, Kindly try after some time.

5. (Optional) To view the logs, go to `/swlibrary/reports/generate_report-YYYYMMDDxxxx.log`.

## Viewing the status of the virtual machine report

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.
3. Type the `./generate_report.sh -s` command.

If the virtual machine report generation is in progress, the system displays the following message: Report Generation Process is Running.

## Aborting the virtual machine report generation

### About this task

If the virtual machine report generation process is in progress and you want to abort the report generation process, use the following procedure.

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Go to the `/swlibrary/reports/` directory.

3. Type the `./generate_report.sh -a` command.

The system aborts the virtual machine report generation process.

---

## Monitoring a host and virtual machine

### Monitoring a platform

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click **Monitor Platforms**.
3. On the Monitor Hosts page, do the following:
  - a. In **Hosts**, click a host.
  - b. Click **Generate Graph**.

The system displays the graph regarding the CPU/memory usage of the host that you selected.

### Monitoring an application

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click **Monitor Applications**.
3. In the Monitor VMs page, do the following:
  - a. In **Hosts**, click a host.
  - b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

---

## Managing vCenter

### Creating a role for a user

#### About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

## Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration > Roles**.  
The system displays the Create Role dialog box.
3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.

- a. In All Privileges, select the following check boxes:

- **Datastore**
- **Datastore cluster**
- **Distributed switch**
- **Folder**
- **Host profile**
- **Network**
- **Resource**
- **Tasks**
- **Virtual machine**
- **vApp**

 **Note:**

You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

- b. In All Privileges, expand **Host**, and select the **Configuration** check box.

 **Note:**

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

## Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

## Adding a vCenter to Solution Deployment Manager

### About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, and 7.0. When you add vCenter, System Manager discovers the ESXi hosts that this

vCenter manages, adds to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository. System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

### Before you begin

Ensure that you have the required permissions.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
  - a. In **vCenter FQDN**, type FQDN of vCenter.
    - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
    - The FQDN value must match with the value of the **SAN** field of the vCenter certificate. The FQDN value is case sensitive.
  - b. In **User Name**, type the user name to log in to vCenter.
  - c. In **Password**, type the password to log in to vCenter.
  - d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.
 

If you select the authentication type as **SSO**, the system displays the **Is SSO managed by Platform Service Controller (PSC)** field.
  - e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.
 

PSC must have a valid certificate.

The system enables **PSC IP or FQDN** and you must provide the IP or FQDN of PSC.
  - f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

The system generates the certificate and adds vCenter.

In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

### Related links

[Editing vCenter](#) on page 1380

[Map vCenter field descriptions](#) on page 1381

[New vCenter and Edit vCenter field descriptions](#) on page 1381

## Editing vCenter

### Before you begin

Ensure that you have the required permissions.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select a vCenter server and click **Edit**.
4. In the Edit vCenter section, change the vCenter information as appropriate.
5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then click **Accept Certificate**.
6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
  - Select an ESXi host and click the edit icon (✎).
  - Select one or more ESXi hosts, select the location, click **Bulk Update > Update**.
7. Click **Commit** to get an updated list of managed and unmanaged hosts.

If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged Hosts or vice versa, and you refresh the table, the page displays the same host in both the tables.

## Deleting vCenter from Solution Deployment Manager

### Before you begin

Ensure that you have the required permissions.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
4. Click **Yes** to confirm the deletion of servers.

The system deletes the vCenter from the inventory.

## Map vCenter field descriptions

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>               | The name of the vCenter server.                                                                                                                                                                                                                                                                                                                                                |
| <b>IP</b>                 | The IP address of the vCenter server.                                                                                                                                                                                                                                                                                                                                          |
| <b>FQDN</b>               | <p>The FQDN of the vCenter server.</p> <p> <b>Note:</b></p> <p>Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.</p>                          |
| <b>License</b>            | The license type of the vCenter server.                                                                                                                                                                                                                                                                                                                                        |
| <b>Status</b>             | The license status of the vCenter server.                                                                                                                                                                                                                                                                                                                                      |
| <b>Certificate Status</b> | <p>The certificate status of the vCenter server. The options are:</p> <ul style="list-style-type: none"> <li>: The certificate is correct.</li> <li>: The certificate is not accepted or invalid.</li> </ul> |

| Button                             | Description                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View</b>                        | Displays the certificate status details of the vCenter server.                                                                                                                                    |
| <b>Generate/Accept Certificate</b> | <p>Displays the certificate dialog box where you can generate and accept a certificate for vCenter.</p> <p>For vCenter, you can only accept a certificate. You cannot generate a certificate.</p> |

| Button         | Description                                                                                 |
|----------------|---------------------------------------------------------------------------------------------|
| <b>Add</b>     | Displays the New vCenter page where you can add a new ESXi host.                            |
| <b>Edit</b>    | Displays the Edit vCenter page where you can update the details and location of ESXi hosts. |
| <b>Delete</b>  | Deletes the ESXi host.                                                                      |
| <b>Refresh</b> | Updates the list of ESXi hosts in the Map vCenter section.                                  |

## New vCenter and Edit vCenter field descriptions

| Name                | Description                                     |
|---------------------|-------------------------------------------------|
| <b>vCenter FQDN</b> | The FQDN of vCenter.                            |
| <b>User Name</b>    | The user name to log in to vCenter.             |
| <b>Password</b>     | The password that you use to log in to vCenter. |

*Table continues...*

| Name                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authentication Type</b>                                 | <p>The authentication type that defines how Solution Deployment Manager performs user authentication. The options are:</p> <ul style="list-style-type: none"> <li>• <b>SSO</b>: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server.</li> <li>• <b>LOCAL</b>: User created in vCenter</li> </ul> <p>If you select the authentication type as <b>SSO</b>, the system displays the <b>Is SSO managed by Platform Service Controller (PSC)</b> field.</p> |
| <b>Is SSO managed by Platform Service Controller (PSC)</b> | The check box to specify if PSC manages SSO service. When you select the check box, the system enables <b>PSC IP or FQDN</b> .                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>PSC IP or FQDN</b>                                      | The IP or FQDN of PSC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Button         | Description                                                                       |
|----------------|-----------------------------------------------------------------------------------|
| <b>Save</b>    | Saves any changes you make to FQDN, username, and authentication type of vCenter. |
| <b>Refresh</b> | Refreshes the vCenter details.                                                    |

## Managed Hosts

| Name                | Description                                                           |
|---------------------|-----------------------------------------------------------------------|
| <b>Host IP/FQDN</b> | The name of the ESXi host.                                            |
| <b>Host Name</b>    | The IP address of the ESXi host.                                      |
| <b>Location</b>     | The physical location of the ESXi host.                               |
| <b>IPv6</b>         | The IPv6 address of the ESXi host.                                    |
| <b>Host Path</b>    | The hierarchy of the host in vCenter and also includes the host name. |

| Button             | Description                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Edit</b>        | The option to edit the location and host.                                                                                                                                                                                                                 |
| <b>Bulk Update</b> | <p>Provides an option to change the location of more than one ESXi hosts.</p> <p> <b>Note:</b><br/>You must select a location before you click <b>Bulk Update</b>.</p> |
| <b>Update</b>      | Saves the changes that you make to the location or hostname of the ESXi host.                                                                                                                                                                             |
| <b>Commit</b>      | Commits the changes that you make to the ESXi host with location that is managed by vCenter.                                                                                                                                                              |

## Unmanaged Hosts

| Name                | Description                |
|---------------------|----------------------------|
| <b>Host IP/FQDN</b> | The name of the ESXi host. |

*Table continues...*



| Name                | Description                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ESXi Version</b> | Displays the versions of the ESXi host linked to <b>vCenter FQDN</b> .<br><br>* <b>Note:</b><br>For Release 8.1 and later, do not select the 5.0 and 5.1 versions. |
| <b>IPv6</b>         | The IPv6 address of the ESXi host.                                                                                                                                 |
| <b>Host Path</b>    | The hierarchy of the host in vCenter and also includes the host name.                                                                                              |

| Button        | Description                                                         |
|---------------|---------------------------------------------------------------------|
| <b>Commit</b> | Saves all changes that you made to vCenter on the Map vCenter page. |

## Managing syslog profiles

### Adding a remote Syslog server profile

#### About this task

Use this procedure to configure a remote Syslog server details in System Manager such that it receives system logs from Appliance Virtualization Platform host through AVP Utilities.

#### Before you begin

To view the Syslog data from AVP Utilities or application, ensure that:

- The firewall on the Syslog server is configured correctly.
- The Syslog service on the server is running.

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. Click **Application Management**.
3. In the lower pane, click **Configure Remote Syslog Profile**.
4. On the Syslog Receiver Configuration page, click **Add**.  
System Manager displays the Add Syslog Receiver dialog box
5. In **Profile Name**, type the profile name of the Syslog server.
6. In **IP/FQDN**, type the IP address or FQDN of the Syslog server.
7. In **Port**, type the port of the Syslog server.
8. In **Protocol**, click **TCP** or **UDP**.
9. If the remote host is TLS based, select **TLS Authentication**.
10. In **Authentication options**, click **Server certificate authentication** or **Mutual TLS authentication**.

11. Click **Save**.

## Syslog Receiver Configuration field descriptions

| Name                                     | Description                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile Name</b>                      | The name of the Syslog server configuration.                                                                                                                                                                                                                                                                                                                 |
| <b>IP/FQDN</b>                           | The IP address or host name of the Syslog server configuration.                                                                                                                                                                                                                                                                                              |
| <b>Port</b>                              | The port number of the Syslog server configuration.<br>The default port is 514.                                                                                                                                                                                                                                                                              |
| <b>Protocol</b>                          | The type of port used for the Syslog server configuration.<br>The options are: <ul style="list-style-type: none"> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> </ul> When the <b>tcp</b> protocol is selected, the system enables the <b>TLS Authentication</b> option.                                                                                       |
| <b>TLS Authentication</b>                | The option to select if the remote host is TLS based.<br>When <b>TLS Authentication</b> is selected, the system displays the following options: <ul style="list-style-type: none"> <li>• <b>Server certificate authentication</b></li> <li>• <b>Mutual TLS authentication</b></li> </ul> When you select <b>TLS Authentication</b> , the port value is 6514. |
| <b>Server certificate authentication</b> | The server certificate authentication.<br>This option is available, if <b>TLS Authentication</b> is selected.                                                                                                                                                                                                                                                |
| <b>Mutual TLS authentication</b>         | The mutual certificate authentication.<br>This option is available, if <b>TLS Authentication</b> is selected.                                                                                                                                                                                                                                                |

| Button        | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Add</b>    | Displays the Add Syslog Receiver dialog box where you can add the Syslog server configuration.                  |
| <b>Edit</b>   | Displays the Add Syslog Receiver dialog box where you can edit the configuration of the selected Syslog server. |
| <b>Delete</b> | Deletes the selected Syslog server configuration.                                                               |

## Pushing system logs to Syslog servers

### About this task

Use this procedure to send log files to Syslog servers.

From Release 8.1, you can push more than one Syslog profiles to Syslog servers

## Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions > Syslog config > Push**.
5. In the Push Syslog Configuration dialog box, select one or more Syslog profile, and click **Push**.

The system sends the system log to the selected Syslog server.

## Viewing configured Syslog servers

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions > Syslog config > View**.
5. In the View Syslog Configuration dialog box, select the required Syslog profile to view it.

## Deleting configured Syslog servers

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Host <host name> area, select an application.
4. Click **More Actions > Syslog config > Delete**.
5. In the Delete Syslog Configuration dialog box, select the required Syslog profile, and click **Delete**.
6. On the confirmation dialog box, click **Yes**.

---

## Viewing the job history of virtual machine operations

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the desktop, click the SDM icon () , and then click **Application Management**.
3. In the lower pane, click **Job History**.
4. On the Job History page, in **Operation**, select one or more operations.
5. Click **Submit**.

The page displays the details of jobs that you selected.

### Related links

[Job History field descriptions](#) on page 1391

---

## Application Management field descriptions

| Name                                           | Description                                                                                                                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto-Reload Application Management Tree</b> | The option to automatically reload Application Management Tree after completing an operation, such as refreshing applications. |

### Locations

| Name                 | Description                                |
|----------------------|--------------------------------------------|
| <b>Location Name</b> | The location name.                         |
| <b>City</b>          | The city where the platform is located.    |
| <b>Country</b>       | The country where the platform is located. |

| Button        | Description                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>New</b>    | Displays the New Location section where you can provide the details of the location that you want to add.                               |
| <b>Edit</b>   | Displays the Edit Location section where you can change the details of an existing location.                                            |
| <b>Delete</b> | Deletes the locations that you select.<br><br>The system moves the platforms associated with the deleted locations to unknown location. |

## Platforms

| Name                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Platform Name</b>               | The name of the platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Platform IP</b>                 | The IP address of the platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Platform FQDN</b>               | The FQDN of the platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IPv6</b>                        | The IPv6 address of the platform.<br><br>If the IP address of the ESXi platform only supports IPv4, the column does not display any value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>vCenter FQDN</b>                | The FQDN of vCenter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Current Action</b>              | The operation that is currently being performed on the platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Last Action</b>                 | The last operation completed on the platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>License Status</b>              | The status of the license.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Platform Version</b>            | The platform version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Offer Type</b>                  | The platform type. The options are: <ul style="list-style-type: none"> <li>• <b>AVP</b>: An Appliance Virtualization Platform platform</li> <li>• <b>Customer VE</b>: A customer-provided VMware ESXi platform</li> <li>• <b>SWONLY</b>: A customer-provided operating system platform</li> </ul>                                                                                                                                                                                                                                                                                                                       |
| <b>SSH Status</b>                  | The SSH service status. The values are enabled and disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Platform Certificate Status</b> | The certificate status of Appliance Virtualization Platform or standalone ESXi. If the ESXi is managed by vCenter, the system displays the value of this field as NA. The options are: <ul style="list-style-type: none"> <li>• : The certificate is added in Solution Deployment Manager and is correct.</li> <li>• : The certificate is not accepted or is invalid.</li> </ul> You can click <b>View</b> for details of the certificate status. |
| <b>vCenter Certificate Status</b>  | The certificate status of the ESXi host. The options are: <ul style="list-style-type: none"> <li>• : The certificate is correct.</li> </ul> The system enables all the options in <b>More Actions</b> that apply to VMware ESXi host. <ul style="list-style-type: none"> <li>• : The certificate is not accepted or is invalid.</li> </ul> You can click <b>View</b> for details of the certificate status.                                       |

### **Note:**

Depending on the Appliance Virtualization Platform host and vCenter certificate status, the system enables the options in **More Actions**.

| Button                                                    | Description                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto Refresh</b>                                       | Automatically refreshes the page with the latest changes. For example, the page updates: <ul style="list-style-type: none"> <li>• The Application state when an application changes.</li> <li>• The license status or certificate status of the platform when the platform changes.</li> </ul> The system refreshes the data every minute. |
| <b>Add</b>                                                | Displays the <b>Add Platform</b> section where you can provide the details of the platform that you want to add.                                                                                                                                                                                                                           |
| <b>Edit</b>                                               | Displays the Platform Information section where you can change the details of an existing platform.                                                                                                                                                                                                                                        |
| <b>Remove</b>                                             | Removes the platforms that you select only from the Solution Deployment Manager client.<br><br>The system moves the platforms associated with the deleted locations to an unknown location.                                                                                                                                                |
| <b>Change Network Params &gt; Change Host IP Settings</b> | Displays the Host Network/IP Settings section where you can change the host IP settings for the Appliance Virtualization Platform host.                                                                                                                                                                                                    |
| <b>Change Network Params &gt; Change Network Settings</b> | Displays the Host Network Setting section where you can change the network settings for the Appliance Virtualization Platform host.                                                                                                                                                                                                        |
| <b>Refresh</b>                                            | Refreshes the status of the platforms.                                                                                                                                                                                                                                                                                                     |
| <b>More Actions &gt; AVP Update/ Upgrade Management</b>   | Displays the Update host page where you can provide the Appliance Virtualization Platform patch file for updating the Appliance Virtualization Platform host.                                                                                                                                                                              |
| <b>More Actions &gt; Change Password</b>                  | Displays the Change Password section where you can change the password for the Appliance Virtualization Platform host.                                                                                                                                                                                                                     |
| <b>More Actions &gt; SSH &gt; Enable SSH</b>              | Enables SSH for the Appliance Virtualization Platform host.<br><br>When enabled successfully, the system displays <code>SSH enabled successfully</code> .                                                                                                                                                                                  |
| <b>More Actions &gt; SSH &gt; Disable SSH</b>             | Disables SSH on the Appliance Virtualization Platform host.<br><br>When disabled, the system displays <code>Disabling SSH for AVP host with &lt;IP address&gt; &lt;FQDN&gt;, &lt;username&gt;</code> .                                                                                                                                     |
| <b>More Actions &gt; Syslog config &gt; Push</b>          | Displays the Push Syslog Configuration section where you can push the syslog configuration on the application host. Syslog is only for Appliance Virtualization Platform. You can select multiple platforms and Push syslog configuration on selected platforms.                                                                           |
| <b>More Actions &gt; Syslog config &gt; View</b>          | Displays the View Syslog Configuration section where you can view syslog profiles of selected Appliance Virtualization Platform platforms.                                                                                                                                                                                                 |
| <b>More Actions &gt; Syslog config &gt; Delete</b>        | Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.                                                                                                                                                                                                                               |

*Table continues...*

| Button                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Actions &gt; Lifecycle Actions &gt; Host Restart</b>          | Restarts the platform and applications that are running on the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>More Actions &gt; Lifecycle Actions &gt; Host Shutdown</b>         | Shuts down the platform and applications that are running on the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>More Actions &gt; Generate/Accept Certificate</b>                  | <p>Displays the Certificate dialog box where you can manage certificates for the platform.</p> <p>Depending on the platform type, the options are:</p> <ul style="list-style-type: none"> <li>• <b>Generate Certificate:</b> To generate a certificate for the Appliance Virtualization Platform host only.</li> <li>• <b>Accept Certificate:</b> To accept a valid certificate for the platform or vCenter.</li> <li>• <b>Decline Certificate:</b> To decline the certificate for the Appliance Virtualization Platform host only. You must regenerate the certificate and accept if you decline a platform certificate.</li> </ul> |
| <b>More Actions &gt; AVP Cert. Management &gt; Manage Certificate</b> | Displays the Load Certificate dialog box from where you can view/generate certificates for Appliance Virtualization Platform hosts, and download them. You can also upload and push third-party signed certificates to the selected platform.                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>More Actions &gt; AVP Cert. Management &gt; Generic CSR</b>        | Displays the Create/Edit CSR dialog box from where you create or edit the generic CSR data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>More Actions &gt; Snapshot Manager</b>                             | Displays the Snapshot Manager dialog box from where you can view and delete the application snapshot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>More Actions &gt; WebLM Configuration</b>                          | Displays the WebLM Configuration dialog box from where you configure WebLM Server for an Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>More Actions &gt; AVP Firewall Rules</b>                           | Displays the Firewall Settings dialog box from where you can view the firewall rules details for an Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>More Actions &gt; Set Login Banner</b>                             | <p>Displays the Message of the Day dialog box from where you can push the login banner text to the selected platform.</p> <p> <b>Note:</b></p> <p>This feature is only available in System Manager Solution Deployment Manager. Solution Deployment Manager Client does not support <b>Set Login Banner</b>.</p>                                                                                                                                                                                                                                  |

## Applications

| Name                    | Description                                  |
|-------------------------|----------------------------------------------|
| <b>Application Name</b> | The name of the application.                 |
| <b>Application IP</b>   | The IP address of the application.           |
| <b>Application FQDN</b> | The FQDN of the application.                 |
| <b>Application IPv6</b> | The IPv6 address of the application, if any. |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>App Name</b>              | The name of the application. For example, Session Manager.                                                                                                                                                                                                                                                                                                                                                  |
| <b>App Version</b>           | The version of the application. For example, 8.1.                                                                                                                                                                                                                                                                                                                                                           |
| <b>Application State</b>     | The state of the application. The states are: <ul style="list-style-type: none"> <li>• <b>Started</b></li> <li>• <b>Stopped</b></li> </ul>                                                                                                                                                                                                                                                                  |
| <b>Current Action Status</b> | The status of the current operation. The options are: <ul style="list-style-type: none"> <li>• <b>Deploying</b></li> <li>• <b>Starting</b></li> <li>• <b>Stopping</b></li> </ul> The <b>Status Details</b> link provides the details of the operation in progress.                                                                                                                                          |
| <b>Last Action</b>           | The last action performed on the application.                                                                                                                                                                                                                                                                                                                                                               |
| <b>Platform Name</b>         | The platform name of the operating system, VMware host, or Appliance Virtualization Platform host on which the application resides.                                                                                                                                                                                                                                                                         |
| <b>Trust Status</b>          | The status of the connection between System Manager and the application.<br>The options are: <ul style="list-style-type: none"> <li>• <b>Success</b></li> <li>• <b>Failed</b></li> </ul> When the connection between System Manager and the application is established, <b>Trust Status</b> changes to <b>Success</b> .<br>Only when the trust status is <b>Success</b> , you can perform other operations. |
| <b>Data Store</b>            | The data store name.                                                                                                                                                                                                                                                                                                                                                                                        |

| Button                                               | Description                                                                                                           |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>New</b>                                           | Displays the Application Deployment section where you can provide the platform and deploy an application.             |
| <b>Edit</b>                                          | Displays the Application Deployment section where you can change the details of an application.                       |
| <b>Delete</b>                                        | Turns off the applications and deletes the selected application from platform and Solution Deployment Manager Client. |
| <b>Start</b>                                         | Starts the selected applications.                                                                                     |
| <b>Stop</b>                                          | Stops the selected applications.                                                                                      |
| <b>Show Selected</b>                                 | Displays only the selected applications.                                                                              |
| <b>VM Console &gt; Open VM Console in New Window</b> | Opens the application VM console in the new browser window.                                                           |
| <b>VM Console &gt; Open VM Console in New Tab</b>    | Opens the application VM console in the new tab of the browser.                                                       |

*Table continues...*



| Button                                             | Description                                                                                                                        |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Actions &gt; Restart</b>                   | Starts the selected applications that were stopped earlier.                                                                        |
| <b>More Actions &gt; Refresh App</b>               | Updates the status of the applications.                                                                                            |
| <b>More Actions &gt; Re-establish connection</b>   | Establishes the connection between System Manager and the application.<br>The <b>Trust Status</b> then changes to <b>Success</b> . |
| <b>More Actions &gt; Update Static Routing</b>     | Displays the VM Update Static Routing section where you can update the IP address of AVP Utilities for static routing.             |
| <b>More Actions &gt; Syslog config &gt; Push</b>   | Displays the Push Syslog Configuration section where you can push the syslog configuration on the selected application.            |
| <b>More Actions &gt; Syslog config &gt; View</b>   | Displays the View Syslog Configuration section where you can view all configured syslog profiles.                                  |
| <b>More Actions &gt; Syslog config &gt; Delete</b> | Displays the Delete Syslog Configuration section where you can select and delete configured syslog profiles.                       |

## Job History field descriptions

| Name/Button      | Description                                                                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operation</b> | The operation that is performed on a virtual machine.<br>You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation. |
| <b>Submit</b>    | Provides details of jobs that you selected.                                                                                                                                                                       |

### History

| Name              | Description                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job ID</b>     | The unique name of the virtual machine management job.                                                                                 |
| <b>IP/FQDN</b>    | The IP address or host name of the virtual machine or the host where the operation is performed.                                       |
| <b>Operation</b>  | The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation. |
| <b>Status</b>     | The status of the job.                                                                                                                 |
| <b>Start Time</b> | The start time of the job.                                                                                                             |
| <b>End Time</b>   | The end time of the job.                                                                                                               |

---

# Upgrading Avaya Aura® applications

---

## Upgrade Management overview

Upgrade Management in Solution Deployment Manager is a centralized upgrade solution of System Manager, provides an automatic upgrade of Avaya Aura® applications. You can upgrade Communication Manager, Session Manager, and Branch Session Manager directly to Release 8.1.3 from a single view. Communication Manager includes associated devices, such as Gateways, TN boards, and media modules. The centralized upgrade process minimizes repetitive tasks and reduces the error rate.

### Important:

- System Manager Release 7.x and later also support the System Manager Release 6.3.8 flow to upgrade Communication Manager, gateways, media modules, and TN boards to Release 6.3.100. However, the Release 6.3.8 user interface is available only when you select **Release 6.3.8** as the target version on the Upgrade Release Selection page.
- Ensure that upgrade or update of host should not be simultaneously run with upgrade and updates of application. You can check the Job status on the **Home > Services > Solution Deployment Manager > Upgrade Jobs Status** page. Any scheduled, pending, or running jobs for host must be completed before performing upgrade or update operations on host.

With Upgrade Management, you can perform the following:

1. Refresh elements: To get the current state or data such as current version of the Avaya Aura® application. For example, for Communication Manager, gateways, media modules, and TN boards.
2. Analyze software: To analyze whether the elements and components are on the latest release and to identify whether a new software is available for the inventory that you collected.

### Note:

In Geographic Redundancy configured System Manager, if Communication Manager or LSP has the **Unknown** status in the **Managed By** column on the **Inventory > Manage Elements** page, then you cannot perform the analyze operation. To change the **Unknown** status in the **Managed By** column to either **Primary** or **Secondary** depending upon from which system this action is performed, select the entry on the **Inventory > Manage Elements** page, and click **More Actions > Manage**.

3. Download files: To download files that are required for upgrading applications.

You can download a new release from Avaya PLDS to the software file library and use the release to upgrade the device software.

4. Preupgrade check: To ensure that conditions for successful upgrade are met. For example, checks whether:

- The new release supports the hardware
- The RAID battery is sufficient
- The bandwidth is sufficient

**\* Note:**

You must have the minimum network speed of 2Mbps with up to 100ms delay (WAN).

- The files are downloaded

5. Upgrade applications: To upgrade Avaya Aura® applications to Release 8.1.3.

6. Install patches: To install the software patches, service packs, and feature pack.

### Upgrade automation level

- The upgrade of Communication Manager, Session Manager, Branch Session Manager, and AVP Utilities to Release 8.1.3 is automated. The upgrade process includes creating a backup, deploying OVA, upgrading, installing software patches, feature packs, or service packs, and restoring the backup.
- Upgrade of all other Avaya Aura® applications that Solution Deployment Manager supports can automatically deploy OVA files.

However, the upgrade process involves some manual operations for creating backup, installing patches, and restoring the backup data.

### Upgrade job capacity

System Manager Solution Deployment Manager supports simultaneous upgrades or updates of Avaya Aura® applications. Solution Deployment Manager supports the following upgrade capacity:

- 5 upgrade or update job groups: Multiple applications combined together in an upgrade or update job is considered a group.
- 20 applications in a job group: Maximum applications that can be combined in an upgrade or update job group is 20. You can combine any application type for upgrade in a group.

The capacity also includes applications that are in the paused state. If five upgrade job groups are running or are in a paused state, you cannot upgrade the sixth group.

---

## Avaya Aura® applications upgrade

With System Manager Solution Deployment Manager, you can upgrade the following Avaya Aura® applications to Release 8.1.3:

- Communication Manager
- Session Manager
- Branch Session Manager

- AVP Utilities
- WebLM



**Note:**

You must upgrade System Manager to Release 8.1.3 by using the Solution Deployment Manager client before you upgrade the Avaya Aura® applications to Release 8.1.3.

**Related links**

[Guidelines for upgrading and updating elements](#) on page 1394

## Guidelines for upgrading and updating elements

### Upgrading elements

For System Manager that is on the latest major release, to upgrade the elements to an intermediate element release, download the latest recommended major release of element OVA in the software library.

For example, for System Manager Release 8.0, to upgrade Communication Manager Release 7.0 to Release 7.1, download Release 8.0 Communication Manager OVA in the software library.

### Updating elements

For System Manager that is on the latest release patch, to upgrade the elements to an intermediate element patch release, download the latest recommended major release of element patch in the software library.

For example, for System Manager Release 8.0.1, to upgrade Communication Manager Release 7.0 to Release 7.1.2, download patch Release 7.1.3 in the software library.

**Related links**

[Avaya Aura applications upgrade](#) on page 1393

---

## Upgrade checklist for Avaya Aura® Virtual Appliance

This is a reference checklist for Virtual Appliance. For detailed steps, see the application specific upgrading guides.

| Nos. | Tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Notes                                                                                               | ✓ |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---|
| 1    | <p>Download the OVA files, ISO files, and feature pack files of Avaya Aura® applications that you want to deploy or upgrade from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</p> <p> <b>Note:</b></p> <p>For information about the upgrade sequence and the required patches, see the latest <i>Avaya Aura® Release Notes</i> for the specific release on the Avaya Support website.</p> | -                                                                                                   |   |
| 2    | <p>If you need to deploy or upgrade the System Manager, do the following:</p> <p>Download the Avaya_SDMClient_win64_8.1.3.0.1035538_49.zip file from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.</p>                                                                                                                                                                                                                                                                      | -                                                                                                   |   |
| 3    | <p>Install the Avaya_SDMClient_win64_8.1.3.0.1035538_49.exe file.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -                                                                                                   |   |
| 4    | <p>To upgrade on an Avaya-provided server, use Solution Deployment Manager client for Appliance Virtualization Platform.</p>                                                                                                                                                                                                                                                                                                                                                                                                | -                                                                                                   |   |
| 5    | <p>If System Manager is:</p> <ul style="list-style-type: none"> <li>• Unavailable: On Appliance Virtualization Platform, deploy the System Manager Release 8.1 OVA file, and install the Release 8.1.3 bin file by using the Solution Deployment Manager client.</li> <li>• Available: Upgrade System Manager to 8.1 and install the Release 8.1.3 bin file.</li> </ul>                                                                                                                                                     | -                                                                                                   |   |
| 6    | <p>Discover the applications and associated devices that you want to upgrade by enabling SNMP or manually add the elements from <b>Manage Elements &gt; Discovery</b>.</p>                                                                                                                                                                                                                                                                                                                                                  | For more information, see “Discovering elements” in <i>Administering Avaya Aura® System Manager</i> |   |
| 7    | <p>Configure user settings.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | For more information, see “User settings” in <i>Administering Avaya Aura® System Manager</i>        |   |

Table continues...

| Nos. | Tasks                                                                                                                                                                                             | Notes                                                                                                          | ✓ |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---|
| 8    | Use a local System Manager library or create a remote software library.<br><br>* <b>Note:</b><br>For local, the software local library for TN Boards and media gateway upgrades is not supported. | For more information, see “User settings” in <i>Administering Avaya Aura® System Manager</i>                   |   |
| 9    | Refresh the elements in the inventory.                                                                                                                                                            | For more information, see “Refreshing elements” in <i>Administering Avaya Aura® System Manager</i>             |   |
| 10   | Analyze the software.                                                                                                                                                                             | For more information, see “Analyzing software” in <i>Administering Avaya Aura® System Manager</i>              |   |
| 11   | Perform the preupgrade check.                                                                                                                                                                     | For more information, see “Performing the preupgrade check” in <i>Administering Avaya Aura® System Manager</i> |   |
| 12   | Download the required firmware for the Avaya Aura® application upgrade.                                                                                                                           | For more information, see “Downloading the software” in <i>Administering Avaya Aura® System Manager</i>        |   |
| 13   | Perform the upgrade.                                                                                                                                                                              | -                                                                                                              |   |
| 14   | Verify that the upgrade is successful.                                                                                                                                                            | -                                                                                                              |   |

## Upgrade target release selection

For backward compatibility, System Manager supports upgrading Communication Manager to Release 6.3.6 or later. By default, the target version is set to System Manager 7.0. Based on the entitlements, to upgrade Communication Manager and the associated applications to Release 6.3.6 or later, you must select 6.3.8 as the upgrade target release.

### Related links

[Selecting the target release for upgrade](#) on page 1396

## Selecting the target release for upgrade

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.

3. In the **Upgrade to release** field, select one of the following:

- **SMGR 7.x:** To upgrade Avaya applications to Release 7.0 or later from the Upgrade Management page.
- **SMGR 6.3.8:** To upgrade Communication Manager and the associated applications to Release 6.3.6 or later from the **Upgrade Management > Software Inventory** page.

 **Important:**

By default, the target version is set to Release 7.0.

4. Click **Commit**.
5. Click **OK**.
6. To perform the upgrade, click **Upgrade Management**.

#### Related links

[Upgrade target release selection](#) on page 1396

---

## Installing software patches by using Solution Deployment Manager

### About this task

Use the procedure to install software patches and service packs that are entitled for an Avaya Aura® application, and commit the patches that you installed.

 **Note:**

When you are installing an element patch and the patch installation fails or the patch information is unavailable in **Upgrade Actions > Installed Patches** on the Upgrade Management page, then perform the following:

1. Ensure that the element is reachable on System Manager Solution Deployment Manager.
2. Refresh the element.

### Before you begin

- Perform refresh and analyze operations.
- If you upgrade an application that was not deployed from Solution Deployment Manager:
  1. Select the virtual machine.
  2. To establish trust, click **More Actions > Re-establish Connection**.
  3. Click **Refresh VM**.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.

3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions > Upgrade/Update**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.

 **Note:**

If an application is unreachable, the auto commit operation might fail and the Update Patch Status window displays a warning message. You must wait for some time, select the same patch in the Installed Patches section, and perform the commit operation again.

9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. Click **Save**.
11. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

If the field displays , review the information on the Edit Upgrade Configuration page.

12. Click **Upgrade**.
13. On the Job Schedule page, click one of the following:
  - **Run Immediately**: To perform the job.
  - **Schedule later**: To perform the job at a scheduled time.
14. Click **Schedule**.

On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .

15. To view the update status, click .

The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

When the update is complete, the **Update status** and **Last Action Status** fields displays .

16. Click **Upgrade Actions > Installed Patches**.
17. On the Installed Patches page, in the Patch Operation section, click **Commit**.

The page displays all software patches that you can commit.



You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

18. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

You can schedule to commit the patch at a later time by using the **Schedule later** option.

19. Click **Schedule**.

The Upgrade Management page displays the last action as **Commit**.

20. Ensure that **Update status** and **Last Action Status** fields display .

 **Note:**

If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

---

## Installing custom software patches

### About this task

With this procedure, you can install a single software file, such as software patch, service pack, or a feature pack to an Avaya Aura® application. With the custom patch deployment, you do not require the System Manager automation and analyze functions, so that the advanced administrators can fully control the deployment of hot fixes, patches, service pack, and feature packs.

You can install custom patches for the following Avaya Aura® applications:

- Communication Manager
- Session Manager
- Branch Session Manager
- Utility Services
- Communication Manager Messaging
- WebLM
- Application Enablement Services

### Before you begin

Before you begin with installing custom patches, perform refresh and analyze using the following procedures:

- For refreshing elements, see [Refreshing elements](#) on page 1311
- For analyzing elements, see [Analyzing software](#) on page 1311

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.

2. In the navigation pane, click **Upgrade Management**.
3. Select an Avaya Aura® application on which you want to install the patch.
4. Click **Upgrade Actions > Custom Patching**.
5. On the Upgrade Configuration page, click **Edit**.
6. In the General Configuration Details section, in the **Operation** field, click **Update**.
7. In **Upgrade Source**, select the software library where you have downloaded the patch.
8. **(Optional)** Click the **Auto Commit** check box, if you want the system to automatically commit the patch.
9. In the Upgrade Configuration Details section, in the Select patches for update table, select the software patch that you want to install.
10. In the End User License Agreement section, click **I Agree to the above end user license agreement**.
11. Click **Save**.
12. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

If the field displays , review the information on the Edit Upgrade Configuration page.

13. Click **Upgrade**.
14. On the Job Schedule page, click one of the following:
  - **Run Immediately**: To perform the job.
  - **Schedule later**: To perform the job at a scheduled time.
15. Click **Schedule**.

On the Upgrade Management page, the **Update status** and **Last Action Status** fields display .

16. To view the update status, click .

The **Upgrade Job Details** page displays the detailed update checks that are in progress. Click **Done** to close the window.

When the update is complete, the **Update status** and **Last Action Status** fields displays .

17. Click **Upgrade Actions > Installed Patches**.
18. On the Installed Patches page, in the Patch Operation section, click **Commit**.

The page displays all software patches that you can commit.

You can use **Rollback** and **Uninstall** options if you must rollback and uninstall the software patch.

19. Select the patch that you installed, in the Job Schedule section, click **Run Immediately**.

You can schedule to commit the patch at a later time by using the **Schedule later** option.

20. Click **Schedule**.

The Upgrade Management page displays the last action as **Commit**.

21. Ensure that **Update status** and **Last Action Status** fields display .

 **Note:**

If the patch commit fails or auto commit is not executed even after 24 hours, delete the snapshot that are not required. For information about deleting the virtual machine snapshot from host, see “Deleting the virtual machine snapshot”.

## Installed Patches field descriptions

| Name             | Description                                              |
|------------------|----------------------------------------------------------|
| <b>Commit</b>    | The option to select the patches that you can commit.    |
| <b>Uninstall</b> | The option to select the patches that you can uninstall. |
| <b>Rollback</b>  | The option to select the patches that you can rollback.  |
| <b>Show All</b>  | The option to display all the available options.         |

| Name                 | Description                                                                                                                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>          | The name of the software patch.                                                                                                                                                                                                          |
| <b>Element Name</b>  | The element on which the software patch is installed.                                                                                                                                                                                    |
| <b>Patch Version</b> | The version of the software patch.                                                                                                                                                                                                       |
| <b>Patch Type</b>    | The type of the software patch. The options are: <ul style="list-style-type: none"> <li>• service pack or feature pack or software patch</li> <li>• Kernel</li> <li>• Security</li> </ul>                                                |
| <b>Patch State</b>   | The state of the software patch. The options are: <ul style="list-style-type: none"> <li>• Active (when patch is activated)</li> <li>• Installed (when patch is unpacked)</li> <li>• Pending (when patch is pending a commit)</li> </ul> |

| Name                | Description                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Job</b> | The option to schedule a job: <ul style="list-style-type: none"> <li>• <b>Run immediately</b>: To run the upgrade job immediately.</li> <li>• <b>Schedule later</b>: To run the upgrade job at the specified date and time.</li> </ul> |

*Table continues...*

| Name             | Description                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Date</b>      | The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job. |
| <b>Time</b>      | The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.           |
| <b>Time Zone</b> | The time zone of your region.<br><br>This field is available when you select the <b>Schedule later</b> option for scheduling a job.                                                                                     |

| Name            | Description                                                                       |
|-----------------|-----------------------------------------------------------------------------------|
| <b>Schedule</b> | Runs the job or schedules to run at the time that you configured in Job Schedule. |

## Upgrade Management field descriptions

You can apply filters and sort each column in the devices list.

| Name              | Description                                                                     |
|-------------------|---------------------------------------------------------------------------------|
| <b>Name</b>       | The name of the device that you want to upgrade.                                |
| <b>Parent</b>     | The name of the parent of the device.<br>For example, CommunicationManager_123. |
| <b>Type</b>       | The device type.<br>For example, TN board.                                      |
| <b>Sub-Type</b>   | The sub type of the device.<br>For example, TN2302AP.                           |
| <b>IP Address</b> | The IP address of the device.                                                   |

*Table continues...*

| Name                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Release Status</b>           | <p>The release status of the device. The upgrade status can be:</p> <p>For upgrade:</p> <ul style="list-style-type: none"> <li>• : Upgraded successfully</li> <li>• : Ready for upgrade</li> <li>• : Pending execution</li> <li>• : Status unknown</li> <li>• : Upgrade process paused</li> <li>• : Nonupgradable</li> <li>• : Operation failed</li> </ul> |
| <b>Update Status</b>            | <p>The update status of the device. The upgrade status can be:</p> <ul style="list-style-type: none"> <li>• : Upgraded successfully</li> <li>• : Ready for upgrade</li> <li>• : Pending execution</li> <li>• : Status unknown</li> <li>• : Upgrade process paused</li> <li>• : Nonupgradable</li> <li>• : Operation failed</li> </ul>               |
| <b>Last Action</b>              | The last action performed on the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Last Action Status</b>       | The status of the last action that was performed on the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Pre-upgrade Check Status</b> | <p>The status of preupgrade check of the device. The options are:</p> <ul style="list-style-type: none"> <li>• : Mandatory checks and recommended checks passed</li> <li>• : Mandatory checks are successful, but recommended checks failed.</li> <li>• : Mandatory checks and recommended checks failed</li> </ul> <p>You can click the icon to view the details on the Element Check Status dialog box.</p>                                                                                                                                                                                                                                                                            |
| <b>Current Version</b>          | The software release status of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Entitled Upgrade Version</b> | The latest software release to which the device is entitled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Entitled Update Version</b>  | The latest software patch or service pack to which the device is entitled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Location</b>                 | The location of the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Button                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pre-upgrade Actions &gt; Refresh Elements</b>    | Refreshes the fields that includes the status and version of the device.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Pre-upgrade Actions &gt; Analyze</b>             | Finds if the latest entitled product release is available for a device and displays the report.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Pre-upgrade Actions &gt; Pre-upgrade Check</b>   | Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.                                                                                                                                                                                                                                                                                                                             |
| <b>Upgrade Actions &gt; Upgrade/Update</b>          | Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.                                                                                                                                                                                                                                                                                                                                 |
| <b>Upgrade Actions &gt; Commit/Rollback Upgrade</b> | Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.                                                                                                                                                                                                                                                                                                                                                     |
| <b>Upgrade Actions &gt; Installed Patches</b>       | Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.                                                                                                                                                                                                                                                                                           |
| <b>Upgrade Actions &gt; Custom Patching</b>         | Displays the Upgrade Configuration page where you configure the custom patch details.<br><br>You can then install and commit the custom patch.                                                                                                                                                                                                                                                                                                   |
| <b>Upgrade Actions &gt; Cleanup</b>                 | Clears the current pending or pause state of applications.<br><br>The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade.<br><br>If you continue the cleanup, the system clears the states, and you can start the upgrade process again. |
| <b>Upgrade Actions &gt; Commit</b>                  | Commits the changes that you made.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Upgrade Actions &gt; Rollback</b>                | Resets the system to the previous state.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Upgrade Actions &gt; Resume</b>                  | Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                       |
| <b>Download &gt; Download</b>                       | Displays the File Download Manager page with the list of downloaded software required for upgrade or update.                                                                                                                                                                                                                                                                                                                                     |
| <b>Download &gt; Bulk Import Spreadsheet</b>        | Downloads the <code>Bulk_Import_Spreadsheet_Template.xlsx</code> file on your local computer.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Show Selected Elements</b>                       | Displays only the elements that you selected for preupgrade or update.                                                                                                                                                                                                                                                                                                                                                                           |

## Upgrade Configuration field descriptions

| Name                | Description             |
|---------------------|-------------------------|
| <b>Element Name</b> | The name of the device. |

*Table continues...*

| Name                                       | Description                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parent Name</b>                         | The parent of the device.<br>For example, CommunicationManager_123.                                                                                                                                                                                                                                                |
| <b>Type</b>                                | The device type.                                                                                                                                                                                                                                                                                                   |
| <b>IP Address</b>                          | The IP Address of the device.                                                                                                                                                                                                                                                                                      |
| <b>Current Version</b>                     | The release status of the device.                                                                                                                                                                                                                                                                                  |
| <b>Override Preupgrade Check</b>           | The option to override preupgrade check recommendations.<br><br>When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as <b>Partial_Failure</b> . |
| <b>Override Delete VM on Upgrade Check</b> | The option to override upgrade check recommendations.<br><br>When you select this option, the system deletes the old virtual machine after the upgrade check.                                                                                                                                                      |
| <b>Edit</b>                                | Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.                                                                                                                                                                                                              |
| <b>Configuration Status</b>                | An icon that defines the configuration status.<br><br><ul style="list-style-type: none"> <li>✖: Configuration incomplete.</li> <li>✔: Configuration complete.</li> </ul>                                                                                                                                           |

| Button                         | Description                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Import Configuration(s)</b> | Imports the Bulk_Import_Spreadsheet_Template.xlsx spreadsheet.<br><br>The system displays the Upload Xlsx File Configuration dialog box to upload the Bulk_Import_Spreadsheet_Template.xlsx spreadsheet.                                       |
| <b>Save Configuration</b>      | Saves the upgrade configuration.<br><br> <b>Note:</b><br>The system saves the configuration as a job. You can edit the job on the Upgrade Jobs Status page. |
| <b>Upgrade</b>                 | Commits the upgrade operation.                                                                                                                                                                                                                 |

## Edit Upgrade Configuration field descriptions

Edit Upgrade Configuration has following tabs:

- **Element Configuration**
- **AVP Configuration**

## Element Configuration: General Configuration Details

| Name                                                                 | Description                                                                                                                                                                                                              |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                                                        | The system name.                                                                                                                                                                                                         |
| <b>IP Address</b>                                                    | The IP address of the device.                                                                                                                                                                                            |
| <b>Operation</b>                                                     | The operation that you want to perform on the device. The options are: <ul style="list-style-type: none"> <li>• Upgrade/Migration</li> <li>• Update</li> </ul>                                                           |
| <b>ESXI/AVP host/Platform</b>                                        | The host on which you want to run the device. The options are: <ul style="list-style-type: none"> <li>• Same Box</li> <li>• Software Only</li> <li>• List of hosts that you added from Application Management</li> </ul> |
| <b>New Target ESXI/AVP host/Platform</b>                             | The new target host on which you want to run the device.                                                                                                                                                                 |
| <b>Migrate With AVP Install</b>                                      | The option to migrate System Platform-based Communication Manager Release 6.3.x or 6.4.x to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager.                              |
| <b>Upgrade Source</b>                                                | The source where the installation files are available. The options are: <ul style="list-style-type: none"> <li>• SMGR_DEFAULT_LOCAL</li> <li>• Remote Software Library</li> </ul>                                        |
| <b>Upgrade To</b>                                                    | The OVA file to which you want to upgrade.<br><br>When you select the local System Manager library, the system displays the fields and populates most of the data in the Upgrade Configuration Details section.          |
| <b>Service/Feature Pack for auto-install after upgrade/migration</b> | The service pack or feature pack that you want to install.                                                                                                                                                               |

## Element Configuration: Upgrade Configuration Details

The page displays the following fields when you upgrade application and the associated devices. The page displays all values from the existing system. If the system does not populate the values, manually add the values in the mandatory fields.

| Name               | Description                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto Commit</b> | The option to automatically commit the upgrade.<br><br> <b>Note:</b><br>While applying the Communication Manager Security Service Pack (SSP) or Kernel Service Pack (KSP), you must select the <b>Auto Commit</b> check box. |

*Table continues...*



| Name                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Existing Administrative User</b>     | The user name with appropriate admin privileges.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Existing Administrative Password</b> | The password of the administrator.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Pre-populate Data</b>                | The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hostname</b>                         | The IP address of the virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>DNS Search Path</b>                  | The search list of domain names. For example, mydomain.com. Separate the search list names with commas (,).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Password for cust</b>                | The password of the cust user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Password for root</b>                | The password of the root user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Timezone</b>                         | The timezone of the virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>NTP server(s)</b>                    | The IP Address or FQDN of the NTP server. Separate the IP addresses with commas (,).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>EASG User Access</b>                 | <p><b>Enable: (Recommended)</b></p> <p>By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.</p> <p>In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (<a href="http://support.avaya.com/registration">support.avaya.com/registration</a>) for additional information for registering products and establishing remote access and alarming.</p> <p><b>Disable</b></p> <p>By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.</p> <p>Enter 1 to Enable EASG (Recommended) or 2 to <b>Disable</b> EASG.</p> |
| <b>Default Gateway</b>                  | The default gateway of the virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>DNS Servers</b>                      | The DNS IP address of the virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Public IP Address</b>                | The IP Address of AE Services virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Public Netmask</b>                   | The network mask of AE Services virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

*Table continues...*

| Name                                     | Description                                                                                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Private IP Address</b>                | This field is optional and can be configured to be used for private network.                                                                                                                                    |
| <b>Private Netmask</b>                   | This field is optional, and can be configured to be used for private network.                                                                                                                                   |
| <b>Out of Band Management Netmask</b>    | The subnet mask of the virtual machine for out of band management.                                                                                                                                              |
| <b>Out of Band Management IP Address</b> | The IP address of the virtual machine for out of band management.<br>The field is optional network interface to isolate management traffic on a separate interface from the inband signaling network.           |
| <b>Flexi Footprint</b>                   | The virtual resources that must be selected based on capacity required for the deployment of OVA. The value depends on the server on which you deploy the OVA.                                                  |
| <b>Public</b>                            | The port number that you must assign to public port group.                                                                                                                                                      |
| <b>Out of Band Management</b>            | The port number that is assigned to the out of band management port group.<br>The field is available only when you select a different host.                                                                     |
| <b>Private</b>                           | The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process.<br>The field is available only when you select a different host. |
| <b>Datastore</b>                         | The datastore on the target ESXi host.<br>The field is available only when you select a different host.                                                                                                         |

## Element Configuration: Data Encryption

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Encryption</b>                 | <p>Enables or disables the data encryption.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>1</b>: To enable the data encryption.</li> <li>• <b>2</b>: To disable the data encryption.</li> </ul> <p> <b>Important:</b></p> <ul style="list-style-type: none"> <li>• An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.</li> <li>• While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled.</li> <li>• <b>On Solution Deployment Manager:</b> When the <b>Data Encryption</b> field is set to 1, the system enables the <b>Encryption Pass-Phrase</b> and <b>Re-enter Encryption Pass-Phrase</b> fields to enter the encryption passphrase.</li> <li>• <b>On vCenter or ESXi:</b> When the <b>Data Encryption</b> field is set to 1, enter the encryption passphrase in the <b>Password</b> and <b>Confirm Password</b> fields.</li> </ul> |
| <b>Encryption Pass-Phrase</b>          | <p>This field is applicable when data encryption is enabled.</p> <p>The passphrase for data encryption.</p> <p>When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules.</p> <p>When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Re-enter Encryption Pass-Phrase</b> | <p>The passphrase for data encryption.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Require Encryption Pass-Phrase at Boot-Time</b> | <p>If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the <b>Require Encryption Pass-Phrase at Boot-Time</b> check box is selected.</p> <p> <b>Important:</b></p> <p>You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application.</p> <p>If you lose the data encryption passphrase, the only option is to reinstall the OVA.</p> <p>If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure.</p> <p>You can also set up the remote key server by using the <b>encryptionRemoteKey</b> command after the deployment of the application.</p> |

### Element Configuration: End User License Agreement

| Name                                                   | Description                                                                                                  |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>I Agree to the above end user license agreement</b> | <p>The end user license agreement.</p> <p>You must select the check box to accept the license agreement.</p> |

### AVP Configuration: Existing Machine Details

| Name                                  | Description                                             |
|---------------------------------------|---------------------------------------------------------|
| <b>Source IP</b>                      | The source IP address.                                  |
| <b>Source Administrative User</b>     | The source user name with appropriate admin privileges. |
| <b>Source Administrative Password</b> | The source password of the administrator.               |
| <b>Source Root User</b>               | The source user name with appropriate root privileges.  |
| <b>Source Root Password</b>           | The source password of the root.                        |

### AVP Configuration: Configuration Details

| Name                  | Description                                                                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Upgrade Source</b> | <p>The source where the installation files are available. The options are:</p> <ul style="list-style-type: none"> <li>• SMGR_DEFAULT_LOCAL</li> <li>• Remote Software Library</li> </ul> |

*Table continues...*

| Name                                         | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Upgrade To</b>                            | The OVA file to which you want to upgrade.<br><br>When you select the local System Manager library, the system displays the fields and populates most of the data in the Configuration Details section.                                                                                                                                                                                           |
| <b>Dual Stack Setup (with IPv4 and IPv6)</b> | Enables or disables the fields to provide the IPv6 addresses.                                                                                                                                                                                                                                                                                                                                     |
| <b>AVP Management IPv4 Address</b>           | IPv4 address for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                      |
| <b>AVP IPv4 Netmask</b>                      | IPv4 subnet mask for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                  |
| <b>AVP Gateway IPv4 Address</b>              | IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.                                                                                                                                                                                                                                                                                  |
| <b>AVP Hostname</b>                          | Hostname for the Appliance Virtualization Platform host.<br><br>The hostname: <ul style="list-style-type: none"> <li>• Can contain alphanumeric characters and hyphen</li> <li>• Can start with an alphabetic or numeric character</li> <li>• Must contain at least 1 alphabetic character</li> <li>• Must end in an alphanumeric character</li> <li>• Must contain 1 to 63 characters</li> </ul> |
| <b>AVP Domain</b>                            | Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.                                                                                                                                                                                                      |
| <b>IPv4 NTP server</b>                       | IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com                                                                                                                                                                                                                                                                                                               |
| <b>Secondary IPv4 NTP Server</b>             | Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.                                                                                                                                                                                                                                                                                                    |
| <b>Main IPv4 DNS Server</b>                  | Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.                                                                                                                                                                                                                                                                                                   |
| <b>Secondary IPv4 DNS server</b>             | Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.                                                                                                                                                                                                                                                                                              |
| <b>AVP management IPv6 address</b>           | IPv6 address for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                      |
| <b>AVP IPv6 prefix length</b>                | IPv6 subnet mask for the Appliance Virtualization Platform host.                                                                                                                                                                                                                                                                                                                                  |
| <b>AVP gateway IPv6 address</b>              | IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.                                                                                                                                                                                                                                                                                  |
| <b>IPv6 NTP server</b>                       | IPv6 address or FQDN of customer NTP server.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Secondary IPv6 NTP server</b>             | Secondary IPv6 address or FQDN of customer NTP server.                                                                                                                                                                                                                                                                                                                                            |
| <b>Main IPv6 DNS server</b>                  | Main IPv6 address of customer DNS server. One DNS server entry in each line.                                                                                                                                                                                                                                                                                                                      |

*Table continues...*

| Name                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Secondary IPv6 DNS server</b>                      | Secondary IPv6 address of customer DNS server. One DNS server entry in each line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Public vLAN ID (Used on S8300E only)</b>           | VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090.<br><br>Use <b>Public VLAN ID</b> only on the S8300E server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Enable Stricter Password (14 char pass length)</b> | The check box to enable or disable the stricter password.<br><br>The password must contain at least 14 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>AVP Super User Admin Password</b>                  | Admin password for Appliance Virtualization Platform.<br><br>The password must contain at least 8 characters and can include alphanumeric characters and @!\$.<br><br>You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Enhanced Access Security Gateway (EASG)</b>        | <b>Enable: (Recommended)</b><br><br>By enabling Avaya Logins you are granting Avaya access to your system.<br>This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.<br>In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site ( <a href="http://support.avaya.com/registration">support.avaya.com/registration</a> ) for additional information for registering products and establishing remote access and alarming.<br><br><b>Disable</b><br><br>By disabling Avaya Logins you are preventing Avaya access to your system.<br>This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.<br><br>Enter 1 to Enable EASG (Recommended) or 2 to <b>Disable</b> EASG. |
| <b>WebLM IP/FQDN</b>                                  | The IP Address or FQDN of WebLM Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>WebLM Port Number</b>                              | The port number of WebLM Server. The default port is 52233.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Button        | Description                                                               |
|---------------|---------------------------------------------------------------------------|
| <b>Save</b>   | Saves the changes that you made to the Edit Upgrade Configuration page.   |
| <b>Cancel</b> | Cancels the changes that you made to the Edit Upgrade Configuration page. |

## Uploading a custom patch

### About this task

If the file size exceeds 300 MB, the upload operation fails.

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the left navigation pane, click **Download Manager**.
3. In **Select Software/Hardware Types**, select the firmware you want to download.  
You can choose either **Tree View** or **List View** to view the software, hardware types.
4. Click **Show Files**.
5. In the **Select Files Download Details** section, enter **My Computer**.
6. Click **Download**.
7. On the Upload File page, enter the details of the patch file you want to upload.
8. Click **Commit**.
9. On the Upload Remote Warning page, perform one of the following actions:
  - Click **Now** to upload the file to the remote software library.
  - Click **Schedule** to upload the file at the scheduled time.
  - Click **Cancel** to cancel the upload file operation and return to the previous page.

## Uploading custom patch field descriptions

| Name                    | Description                                                                 |
|-------------------------|-----------------------------------------------------------------------------|
| <b>Software Library</b> | The remote software library where you want to upload the custom patch file. |

*Table continues...*

| Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Product Family</b>         | The product family to which the file belongs. In a product family, the number of devices are listed.                                                                                                                                                                                                                                                                                                                                               |
| <b>Device Type</b>            | The device type that you can upgrade using the software library file. For example, B5800 and IP Office are the device types for IP Office.                                                                                                                                                                                                                                                                                                         |
| <b>Software Type</b>          | The type of software file which includes firmware and images.                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>File Version</b>           | <p>The software file version that you want to upload. For example, OVA, service pack, and feature pack.</p> <p>Version number is mandatory if you are uploading files, such as OVA, service pack, and feature pack because analyze operation works on version number and the system might have to install the version of the file. Custom patching does not require the analyze operation, and therefore, the file version number is optional.</p> |
| <b>Hardware Compatibility</b> | The hardware compatibility for the file you upload. For IP Office, this field can be null.                                                                                                                                                                                                                                                                                                                                                         |
| <b>File Size (in bytes)</b>   | The file size of the patch file you want to upload.                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>File</b>                   | The patch file you want to upload to the remote software library. Click <b>Choose File</b> to browse to the file you want to upload.                                                                                                                                                                                                                                                                                                               |

| Button        | Description                                                                   |
|---------------|-------------------------------------------------------------------------------|
| <b>Commit</b> | Click to go to the upload file scheduler page.                                |
| <b>Cancel</b> | Click to cancel the upload operation and return to the Download Manager page. |

## Migrating System Platform-based elements or bare metal-based Communication Manager elements

### Migrating Communication Manager 6.3.x or 6.4.x or CM Simplex on survivable remote template to Avaya Aura® Release 8.1.3 with Appliance Virtualization Platform remote deployment

#### About this task

You can perform the remote deployment, if Communication Manager Release 6.3.x or 6.4.x on System Platform is hosted on the server that is supported with Appliance Virtualization Platform. This procedure can be performed only on the same server.

#### **Note:**

To migrate from System Platform-based Communication Manager Release 6.3.x or 6.4.x to Appliance Virtualization Platform 8.1, you need to first migrate to Appliance Virtualization Platform 8.0.1.1, and then update Appliance Virtualization Platform to 8.1. However, during the migration process, Avaya Aura® applications are migrated to 8.1.



Use this procedure to migrate Communication Manager Release 6.3.x or 6.4.x on System Platform to Avaya Aura® Release 8.1.3 in the following configurations:

- Embedded remote template on S8300E CM Simplex with survivable remote template running on Dell™ PowerEdge™ R620, HP ProLiant DL360p G8, Dell™ PowerEdge™ R630, HP ProLiant DL360 G9, or Avaya Solutions Platform 120 Appliance.

Survivable remote template does not contain Communication Manager Messaging and WebLM, and the bulk of the Communication Manager configuration data is transferred from the Communication Manager main server.

- Communication Manager, Utility Services, Branch Session Manager, and SAL or Services VM.

**\* Note:**

- Utility Services must be available on the Communication Manager 6.3.x or 6.4.x or CM Simplex on survivable remote template.
- You must have the minimum network speed of 2Mbps with up to 100ms delay (WAN).
- During manually patching elements, if the System Platform template is broken, then Solution Deployment Manager does not support the upgrade from System Platform-based Communication Manager Release 6.3.x or 6.4.x to 7.1.2 and later.

## Before you begin

- Manually upgrade the System Platform template on the latest Release 6.3.x or 6.4.x. Then upgrade to Release 7.1.2 and later by using Solution Deployment Manager.

**\* Note:**

Remote upgrade is not supported from System Platform-based Communication Manager Release 6.0 to 7.1.2 and later.

- Download the following components from the PLDS website:
  - Appliance Virtualization Platform Release 8.1.x installation file, `avaya-avp-8.1.x.0.0.xx.iso`.
  - Release 8.1 OVA files for System Manager and other Avaya Aura® applications deployed on System Platform.
  - Release 8.1.3 patch file for System Manager and other Avaya Aura® applications.

**\* Note:**

All the latest OVAs of elements that need to be upgraded with the latest AVP ISO must be available in Software library management in Solution Deployment Manager.

- Ensure that System Manager Solution Deployment Manager is available in the solution with appropriate Communication Manager licenses.

## Procedure

1. Create a backup of the following Communication Manager Release 6.3.x or 6.4.x and associated applications in the survivable remote template:
  - a. Communication Manager

- b. SAL or Services VM backup by using SAL or Services VM application utility
  - c. Branch Session Manager
2. Create a System Platform-based backup.

You require the System Platform backup for disaster recovery purposes and to migrate the SAL Services VM data.
3. Record the following Communication Manager embedded main settings for Release 6.3.x or 6.4.x:
  - All IP addresses
  - Subnetwork mask
  - Gateway
  - DNS
  - NTP Server
4. Add System Platform, Communication Manager Release 6.3.x or 6.4.x, and associated applications in System Manager inventory on the **Services > Inventory > Manage Elements** page.

For information about adding these elements, see *Administering Avaya Aura® System Manager*.

Once elements are successfully added, you can view them on the **Services > Solution Deployment Manager > Upgrade Management** page.
5. On the System Manager web console, click **Services > Solution Deployment Manager > Upgrade Management**,
6. Select Communication Manager and associated elements, and then click **Pre-Upgrade Actions > Refresh Element(s)**.
7. On the next page, click **Schedule**.

You can schedule the job now or for a later time.
8. After refresh is done, click **Pre-Upgrade Actions > Analyze**.
9. On the next page, click **Schedule**.

You can schedule the job now or for a later time.
10. After analyze is done, click **Pre-upgrade Actions > Pre-upgrade Check**.

The preupgrade check provides the hardware requirements for Communication Manager 6.3.x or 6.4.x and associated devices that you migrate and checks whether Utility Services is running on the virtual machine.
11. After Pre-upgrade check is done, click **Upgrade Actions > Upgrade/Update**.

Solution Deployment Manager performs the following:

  - Imports the required network settings from System Platform.

- Prompts you to fill the new attributes from OVA that are required for the deployment.
- Creates a backup of Communication Manager Survivable remote template and other virtual machines that are deployed on System Platform.

Solution Deployment Manager does not backup Communication Manager Messaging.

12. On the Upgrade Configuration page, click **edit**.
13. On the Edit Upgrade Configuration page, in **Service/Feature Pack for auto-install after migration**, select the 8.1.3 feature pack.
14. On the **Element Configuration** tab, fill the required fields, and click **Migrate to AVP install**.
15. On the **AVP Configuration** tab, provide the required details.

If you are migrating from Communication Manager Release 6.3.x or 6.4.x, the system displays the following fields preconfigured and prepopulated.

- **Source Root User**
- **Source Root Password**
- **AVP management IPv4 Address:** In this field assign a new IP address to Appliance Virtualization Platform.

16. Click **Save**.
17. To save the configuration, click **Save Configuration**.

The update configuration is saved as a job in the Upgrade Jobs Status page.

18. On the Upgrade Configuration page, click **Upgrade**.
19. To view the upgrade status, perform the following:
  - a. In the navigation pane, click **Upgrade Job Status**.
  - b. In the **Job Type** field, click **Upgrade**.
  - c. Click the upgrade job that you want to view.
20. On the Upgrade Management page, click .

The **Last Action** column displays **Upgrade**, and the **Last Action Status** column displays .

## Next steps

For migrating Communication Manager 6.3.x or 6.4.x S8300E CM Simplex on survivable remote template to Appliance Virtualization Platform, Utility Services element is also automatically migrated to AVP Utilities Release 8.x.

This process takes approximately 2 to 3 hours depending upon the number of elements to be migrated and network speed.

## Migrating System Platform-based system and elements in bulk to Appliance Virtualization Platform remotely by using System Manager Solution Deployment Manager

### About this task

Use this procedure to remotely migrate System Platform-based system and elements in bulk to Appliance Virtualization Platform Release 8.1.3. You can remotely migrate:

- Communication Manager, Branch Session Manager, and Utility Services that are running on System Platform.
- Communication Manager Release 5.2.1 bare metal system.

### Before you begin

- On the Manage Elements page, add the System Platform system and required elements. For information about adding a new element, see *Administering Avaya Aura® System Manager*.
- Refresh the element.
- Analyze the software.
- Perform the pre-upgrade check.
- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.
- Fill the required system details in the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet.

#### **Note:**

If you provide the incorrect data in the spreadsheet, the upgrade might fail.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.  
The system displays the Upgrade Management page.
3. Select the required element.  
When you select an element, the system selects the parent of the element and all child elements of the element in the hierarchy.
4. Click **Upgrade Actions > Upgrade/Update**.
5. On the Upgrade Configuration page, click **Bulk Import Configuration(s)**.
6. On the Upload Xlsx File Configuration dialog box, perform the following:
  - a. Click **Browse** and select the file from the local computer.
  - b. To upload the spreadsheet, click **Upload**.
  - c. Click **Submit**.

The system displays the file size, timestamp, and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.

On the Upgrade Management page, the system displays the message: Please Wait – Saving Import Excel Sheet Configuration .... You must wait until the system stops showing this message.

7. On the Upgrade Management page, click .

The **Configuration Status** column displays .

8. To save the configuration, click **Save Configuration**.

The update configuration is saved as a job in the Upgrade Jobs Status page.

9. On the Upgrade Configuration page, click **Upgrade**.
10. To view the upgrade status, perform the following:
  - a. In the navigation pane, click **Upgrade Job Status**.
  - b. In the **Job Type** field, click **Upgrade**.
  - c. Click the upgrade job that you want to view.

11. On the Upgrade Management page, click .

The **Last Action** column displays **Upgrade**, and **Last Action Status** column displays .

## Sample scenario for filling AVP Bulk Import Spreadsheet Template

### Example

**SP IP Address** is a primary key that is common in all sub sheets. Let us consider the following element details for Setup 1 Avaya Aura® System Platform LSP in Figure 1:

|      | SP-1            | Dom-0          | CM (LSP)               | US                     | BSM                                 |
|------|-----------------|----------------|------------------------|------------------------|-------------------------------------|
| IP   | 148.147.162.100 | 148.147.162.99 | 148.147.162.101        | 148.147.162.102        | 148.147.162.103                     |
| FQDN |                 |                | spcm.smgrdev.avaya.com | spus.smgrdev.avaya.com | sidtsm2.smgrdev.avaya.com           |
|      |                 |                |                        |                        | <a href="#">SIP:148.147.162.104</a> |

Figure 2: Figure 1. Setup 1 – Avaya Aura® System Platform LSP

The corresponding mapping information of Setup 1 in Element\_Info sub sheet is shown in Figure 2:

| SP IP Address   | Elem | Element IP Ad   | Operation      | ESXI   | Mig  | Upgrade Source | Upgrade To                        |
|-----------------|------|-----------------|----------------|--------|------|----------------|-----------------------------------|
| 148.147.162.100 | CM   | 148.147.162.101 | Upgrade/Migrat | Same B | true | SMGR_DEFAULT_L | CM-Simplex-07.1.0.0.532-e65-0.ova |
| 148.147.162.100 | US   | 148.147.162.102 | Upgrade/Migrat | Same B | true | SMGR_DEFAULT_L | US-7.1.0.0.18-e55-379_OVF10.ova   |
| 148.147.162.100 | BSM  | 148.147.162.103 | Upgrade/Migrat | Same B | true | SMGR_DEFAULT_L | BSM-7.1.0.0.710028-e65-01.ova     |

Figure 3: Figure 2. Setup 1 – Element\_Info sub sheet

The corresponding mapping information of Setup 1 in AVP\_Info sub sheet is shown in Figure 3:

| SP IP Address   | Source IP      | Source | Source A | Sour | Source | Upgrade Source | Upgrade To                 |
|-----------------|----------------|--------|----------|------|--------|----------------|----------------------------|
| 148.147.162.100 | 148.147.162.99 | admin  | admin01  | root | root01 | SMGR_DEFAULT_L | avaya-avp-7.1.2.0.0.07.iso |

Figure 4: Figure 3. Setup 1 – AVP\_Info sub sheet

**\* Note:**

For Avaya Aura® System Platform, the **Source IP** and **AVP\_Mgmt\_IPv4\_Address** is the same as **Dom-0 IP**, which is assigned to the target Appliance Virtualization Platform IP after installation.

The corresponding mapping information of Setup 1 in CM\_Prepopulate\_Data sub sheet is shown in Figure 4:

| SP IP Address   | Element IP Address | CM IPv4 Address | CM IPv4 Netmask | CM IPv4 Gateway |
|-----------------|--------------------|-----------------|-----------------|-----------------|
| 148.147.162.100 | 148.147.162.101    | 148.147.162.101 | 255.255.255.0   | 148.147.162.1   |

Figure 5: Figure 4. Setup 1 – CM\_Prepopulate\_Data sub sheet

**\* Note:**

The values added in the **Element IP Address** and **CM IPv4 Address** columns in the above image must be the same as the **Element IP Address** of CM (LSP) in the Figure 1.

The corresponding mapping information of Setup 1 in US\_Prepopulate\_Data sub sheet is shown in Figure 5:

| SP IP Address   | Element IP Ad   | Hostname | Public IP Address | Public Netm   | Public Default |
|-----------------|-----------------|----------|-------------------|---------------|----------------|
| 148.147.162.100 | 148.147.162.102 | us       | 148.147.162.102   | 255.255.255.0 | 148.147.162.1  |

Figure 6: Figure 5. Setup 1 – US\_Prepopulate\_Data sub sheet

**\* Note:**

The values added in the **Element IP Address** and **Public IP Address** columns in the above image must be the same as the **Element IP Address** of US in the Figure 1.

The corresponding mapping information of Setup 1 in BSM\_Prepopulate\_Data sub sheet is shown in Figure 6:

| SP IP Address   | Element IP Ad   | Short H | Network Domain    | IPv4 Address    | Netmask       | Default gate  |
|-----------------|-----------------|---------|-------------------|-----------------|---------------|---------------|
| 148.147.162.100 | 148.147.162.103 | sidtsm1 | smgrdev.avaya.com | 148.147.162.103 | 255.255.255.0 | 148.147.162.1 |

Figure 7: Figure 6. Setup 1 – BSM\_Prepopulate\_Data sub sheet

The values added in the **Element IP Address** and **IPv4 Address** columns in the above image must be the same as the **Element IP Address** of BSM in the Figure 1.

A sample scenario for Setup 2 (Avaya Aura® System Platform) CM Simplex Main:

| Setup-3 (Bare Metal 5.2.1) LSP |      |      |                 |    |     |
|--------------------------------|------|------|-----------------|----|-----|
|                                | SP-3 | Dom0 | CM              | US | BSM |
| IP                             | NA   | NA   | 148.147.162.301 | NA | NA  |

Figure 8: Figure 7. Setup 2 – (Avaya Aura® System Platform) CM Simplex Main



**\* Note:**

For CM Simplex Main, there is no mapping entry in BSM\_Prepopulate\_Data sub sheet.

A sample scenario for Setup 3 (Bare Metal) 5.2.1 LSP in Figure 8:

| Setup-3 (Bare Metal 5.2.1) LSP |      |      |                 |    |     |
|--------------------------------|------|------|-----------------|----|-----|
|                                | SP-3 | Dom0 | CM              | US | BSM |
| IP                             | NA   | NA   | 148.147.162.301 | NA | NA  |

**Figure 9: Figure 8. Setup 3 – (Bare Metal) 5.2.1 LSP**

**\* Note:**

1. In Element\_Info sub sheet, the **SP IP Address** mentioned in column is NA for Bare Metal 5.2.1.
2. In AVP\_Info sub sheet, the **Source IP** is the LSP IP Address. You need to provide a new IP Address for **AVP\_Mgmt\_IPv4\_Address**, which is assigned to the target Appliance Virtualization Platform Host after installation.
3. In CM\_Prepopulate\_Data sub sheet, the **SP IP Address** mentioned in column is NA for Bare Metal 5.2.1.
4. US\_Prepopulate\_Data sub sheet and BSM\_Prepopulate\_Data sub sheet do not have any mapping entry for Bare Metal 5.2.1 LSP.

**\* Note:**

This information is applicable only if you are migrating to Release 7.1.2 and higher.

## Downloading the bulk import spreadsheet template

### About this task

Use the following procedure to download the `Bulk_Import_Spreadsheet_Template.xlsx` file.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, click **Download > Bulk Import Spreadsheet**.

The system downloads the `Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.

## Upgrading Branch Session Manager instances in bulk

### Filling the bulk import spreadsheet for upgrading Branch Session Manager instances in bulk

#### Before you begin

- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.

#### Procedure

1. On the **Element Info** sheet, do the following:
  - a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Branch Session Manager.  
This field supports the AVP and ESXi platforms.
  - b. In **Element Type**, type `BSM`.
  - c. In **Element IP Address**, type the IP Address of Branch Session Manager.
  - d. In **Operation**, type `Upgrade/Migration`.
  - e. In **ESXi/AVP host**, type the host IP Address of Branch Session Manager.  
The value of the field must match with **SP/AVP/ESXi IP Address**.
  - f. In **Migrate with AVP Install**, type `false`.  
For Branch Session Manager, migration is not applicable.
  - g. In **Upgrade Source**, type `SMGR_DEFAULT_LOCAL`.
  - h. In **Upgrade To**, type the upgrade version of Branch Session Manager OVA.  
For example: `BSM-8.1.0.0.xxxxxx-exx-0x.ova`.
  - i. In **EULA**, type `true`.
  - j. **(Optional)** In **ESXi/AVP New**, type the host IP Address of AVP or ESXi.  
This field is not applicable for the same host upgrade. If you want to migrate from one AVP or ESXi host to the other, you must fill the following fields on the **BSM\_Prepopulate\_Data** sheet:
    - **New ESXi datacentre**
    - **New ESXi datastore**
    - **New ESXi deployment type****ESXi/AVP New host IP** on the **AVP\_VM\_MAPPING** sheet.
2. On the **AVP\_Info** sheet, do the following:
  - a. In **SP/AVP/ESXi IP Address**, type the IP Address of AVP or ESXi host.  
You can also fill the new ESXi host here.



- b. In **Source IP**, type the IP Address of the Appliance Virtualization Platform.
- c. In **Upgrade Source**, type the source where the installation files are available.

The options are:

- `SMGR_DEFAULT_LOCAL`
- Remote Software Library

- d. In **Upgrade To**, type the OVA file name to which you want to upgrade.
- e. In **Dual Stack Setup (with IPv4 and IPv6)**, enable or disable the fields to provide the IPv6 addresses.

The options are:

- **true**: To enable the encryption pass-phrase at boot-time.
- **false**: To disable the encryption pass-phrase at boot-time.

- f. In **EASG**, type 1 to enable the EASG.
- g. In **WebLM Port Number**, type the port number of WebLM Server.

The default port is 52233.

- h. In **EULA**, type `true`.

3. On the **CM\_Prepopulate\_Data** sheet, do the following:

- a. In **SP/AVP/ESXi IP Address**, type the IP Address of AVP or ESXi host.  
You can also fill the new ESXi host here.
- b. In **Element IP Address**, type the IP Address of Communication Manager.
- c. In **NTP Server(s)**, type the IP address or FQDN of the NTP server.  
Separate the IP addresses with commas (,). You can type up to three NTP servers.
- d. In **Search Domain List**, type the search list of domain names.  
For example, mydomain.com. Separate the search list names with commas (,).
- e. In **EASG**, type 1 to enable the EASG.
- f. In **Flexi Footprint**, type the footprint of Communication Manager.  
For example, CM Main Max users 1,000.
- g. **(Optional)** In **Customer Root Account Password**, type the customer root password.  
This field is only applicable for DOD build.

 **Note:**

In **Data Encryption**, type 1 to enable. Fill the encryption pass-phrase and type `true` for encryption pass-phrase at boot-time.

4. On the **US\_Prepopulate\_Data** sheet, do the following:

- a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Utility Services.
- b. In **Element IP Address**, type the IP Address of Utility Services.
- c. In **Primary WebLM IP address for Licensing**, type the IP Address or FQDN of WebLM Server.
- d. In **OOBM Mode**, select the Out of Band Management mode in which you want to deploy.

The options are:

- **OOBM\_Enabled**: To enable Out of Band Management.
- **OOBM\_Disabled**: To disable Out of Band Management

- e. In **EASG**, type 1 to enable the EASG.
- f. **(Optional)** In **Customer Root Account Password**, type the customer root password.  
This field is only applicable for DOD build.

 **Note:**

In **Data Encryption**, type 1 to enable. Fill the encryption pass-phrase and type `true` for encryption pass-phrase at boot-time.

5. On the **BSM\_Prepopulate\_Data** sheet, do the following:

- a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Branch Session Manager.
- b. In **Search Domain List**, type `platform.avaya.com`.
- c. In **LSP IP**, type the Communication Manager IP Address.
- d. In **EASG User Access**, type 1 to enable the EASG.
- e. In **Flexi Footprint**, type the footprint of Branch Session Manager.  
For example, BSM Profile 1 Max Devices 1,000.
- f. **(Optional)** In **Customer Root Account Password**, type the customer root password.  
This field is only applicable for DOD build.

 **Note:**

In **Data Encryption**, type 1 to enable. Fill the encryption pass-phrase and type `true` for encryption pass-phrase at boot-time.

6. On the **AVP\_VM\_MAPPING** sheet, do the following:

- a. In **AVP/ESXi IP Address**, type the IP Address of the AVP or ESXi host.  
You can also fill the new ESXi host here.
- b. In **Authentication Type**, type `SSO` or `LOCAL`.
- c. In **PSC URL**, type FQDN of PSC.

7. Save the values in the sheet.

#### Related links

[Downloading the bulk import spreadsheet template](#) on page 1421

## Upgrading Branch Session Manager instances in bulk by using System Manager Solution Deployment Manager

### Before you begin

- On the Manage Elements page, add Branch Session Manager instances. For information about adding a new element, see *Administering Avaya Aura® System Manager*.
- Refresh the element.
- Analyze the software.
- Perform the pre-upgrade check.
- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.
- Fill the required system details in the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet.

#### **Note:**

If you provide the incorrect data in the spreadsheet, the upgrade might fail.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, select Branch Session Manager instances.
4. Click **Upgrade Actions > Upgrade/Update**.
5. On the Upgrade Configuration page, click **Bulk Import Configuration(s)**.
6. On the Upload Xlsx File Configuration dialog box, perform the following:
  - a. Click **Browse** and select the file from the local computer.
  - b. To upload the spreadsheet, click **Upload**.
  - c. When the spreadsheet upload is 100%, click **Submit**.

The system displays the file size, timestamp, and percentage complete for the uploaded file. When the file upload is in-progress, do not navigate away from the page.

On the Upgrade Management page, the system displays the message: `Please Wait - Saving Import Excel Sheet Configuration . . . . You must wait until the system stops showing this message.`

7. On the Upgrade Management page, click .

The **Configuration Status** column displays .

8. To save the configuration, click **Save Configuration**.

The update configuration is saved as a job in the Upgrade Jobs Status page.

9. On the Upgrade Configuration page, click **Upgrade**.
10. To view the upgrade status, perform the following:
  - a. In the navigation pane, click **Upgrade Job Status**.
  - b. In the **Job Type** field, click **Upgrade**.
  - c. Click the upgrade job that you want to view.

11. On the Upgrade Management page, click .

The **Last Action** column displays **Upgrade**, and **Last Action Status** column displays .

## System Manager upgrade management

### Upgrade Management field descriptions

#### Upgrade Elements

| Name                      | Description                                                                                                                                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SMGR Name</b>          | System Manager name.                                                                                                                                                                                            |
| <b>IP/FQDN</b>            | The IP address or the FQDN of System Manager virtual machine.                                                                                                                                                   |
| <b>C-DOM IP/FQDN</b>      | The IP address or the FQDN of console domain.                                                                                                                                                                   |
| <b>Element Type</b>       | The type of the element.                                                                                                                                                                                        |
| <b>Current Version</b>    | The current version of the element.                                                                                                                                                                             |
| <b>Upgrade To Version</b> | The upgrade to version for the element.                                                                                                                                                                         |
| <b>Upgrade Status</b>     | The status of the upgrade process. The status can be <b>Upgrading</b> , <b>Completed</b> , or <b>Failed</b> .<br><br>The <b>Status Details</b> link provides more information about the System Manager upgrade. |
| <b>Last Action</b>        | The last upgrade action.                                                                                                                                                                                        |
| <b>Related VM</b>         |                                                                                                                                                                                                                 |

| Button              | Description                                                                                |
|---------------------|--------------------------------------------------------------------------------------------|
| <b>Add Elements</b> | Displays the Add Element page where you add System Manager.                                |
| <b>Upgrade</b>      | Displays the Upgrade Management page where you upgrade the System Manager virtual machine. |

*Table continues...*

| Button          | Description                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------|
| <b>Edit</b>     | Displays the Edit Element page where you can change the details of System Manager that you added. |
| <b>Delete</b>   | Deletes the System Manager virtual machine.                                                       |
| <b>Commit</b>   | Saves the changes and upgrades the System Manager virtual machine.                                |
| <b>Rollback</b> | Reverts the upgrade of the System Manager virtual machine.                                        |

## Add Element field descriptions

### System Platform: Required C-DOM information

| Name                        | Description               |
|-----------------------------|---------------------------|
| <b>C-DOM IP/FQDN</b>        | The C-DOM IP/FQDN.        |
| <b>C-DOM SSH User Name</b>  | The C-DOM SSH user name.  |
| <b>C-DOM SSH Password</b>   | The C-DOM SSH password.   |
| <b>C-DOM Root User Name</b> | The C-DOM root user name. |
| <b>C-DOM Root password</b>  | The C-DOM root password.  |

### Virtual Machine Platform (6.x): Required Host/VM Details Information

| Name                    | Description                      |
|-------------------------|----------------------------------|
| <b>Hosts</b>            | The host of the virtual machine. |
| <b>Virtual machines</b> | The virtual machine.             |

### System Platform/Virtual Machine Platform (6.x): Required Element Information

| Name                      | Description                                     |
|---------------------------|-------------------------------------------------|
| <b>SMGR IP</b>            | The IP address of System Manager.               |
| <b>SMGR VM NAME</b>       | The name of the System Manager virtual machine. |
| <b>SMGR SSH User Name</b> | The SSH user name of System Manager.            |
| <b>SMGR SSH Password</b>  | The SSH password of System Manager.             |

| Button      | Description                       |
|-------------|-----------------------------------|
| <b>Save</b> | Saves the element that you added. |

## Edit Elements field descriptions

### Required Element information

| Name                      | Description                                 |
|---------------------------|---------------------------------------------|
| <b>SMGR IP</b>            | The IP address of System Manager.           |
| <b>SMGR NAME</b>          | The name of System Manager virtual machine. |
| <b>SMGR SSH User Name</b> | The SSH user name of System Manager.        |
| <b>SMGR SSH Password</b>  | The SSH password of System Manager.         |

### Required C-DOM information

| Name                        | Description              |
|-----------------------------|--------------------------|
| <b>C-DOM IP/FQDN</b>        | The C-DOM IP/FQDN        |
| <b>C-DOM SSH User Name</b>  | The C-DOM SSH user name  |
| <b>C-DOM SSH Password</b>   | The C-DOM SSH password   |
| <b>C-DOM Root User Name</b> | The C-DOM root user name |
| <b>C-DOM Root password</b>  | The C-DOM root password  |

| Button        | Description                         |
|---------------|-------------------------------------|
| <b>Update</b> | Updates the changes to the element. |

## Upgrade Management field descriptions

| Name                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Install on Same Host</b> | <p>The option to select the same or a different server. The options are:</p> <ul style="list-style-type: none"> <li>• Select: To upgrade on the same server.</li> <li>• Clear: To upgrade to a different server.</li> </ul> <p>If you do not select the check box, you must add a new server or select a server from the list to which you want to update.</p> <p> <b>Note:</b></p> <p>When upgrading from System Platform-based System Manager to AVP or ESXi, the system displays this field.</p> |
| <b>Platform FQDN</b>        | <p>The platform FQDN to which you want to upgrade.</p> <p>The system displays the CPU and memory details of the platform in the Capacity Details section.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Application Name</b>     | The application name displayed on the Add Element page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## OVA/ISO Details

| Name                                    | Description                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select the OVA</b>                   | The option to select a .ova file of the virtual machine that is available on System Manager.                                                                                                                                                                                                         |
| <b>OVA file</b>                         | The absolute path to the .ova file of the virtual machine.<br><br>The field is available only when you click <b>Select the OVA from Local SMGR</b> .                                                                                                                                                 |
| <b>Submit File</b>                      | Selects the .ova file of the virtual machine that you want to deploy.<br><br>The field is available only when you click <b>Select the OVA from Local SMGR</b> . The system displays the network configuration details in the Network Parameters section based on the System Manager virtual machine. |
| <b>Flexi Footprint</b>                  | The footprint size supported for the selected server.<br><br>The system validates for the CPU, memory, and other parameters in the Capacity Details section. You must ensure that the status is  .                |
| <b>SMGR Data migration Utility file</b> | The absolute path to the System Manager data migration utility file.<br><br> <b>Note:</b><br>Provide the latest data migration bin that is available for the System Manager release.                                |
| <b>Service Pack or Feature Pack</b>     | The absolute path to the service pack or feature pack.<br><br>For the latest service pack or feature pack, see Avaya Aura® Release Notes on the Avaya Support website at <a href="http://support.avaya.com/">http://support.avaya.com/</a> .                                                         |

## Configuration Parameters

The system populates the values for most of the fields from the 7.x or 8.0.x system. You must provide information, such as password, FQDN, time zone, and EASG.

## Management Network Settings

| Name                                                                    | Description                                                                                                                                                                                                             |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Management IPv4 Address (or Out of Band Management IPv4 Address)</b> | The IPv4 address of the System Manager application for out of band management.<br><br>The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network. |
| <b>Management Netmask</b>                                               | The Out of Band Management subnetwork mask to assign to the System Manager application.                                                                                                                                 |
| <b>Management Gateway</b>                                               | The gateway IPv4 address to assign to the System Manager application.                                                                                                                                                   |
| <b>IP Address of DNS Server</b>                                         | The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).                                                                             |

*Table continues...*

| Name                       | Description                                                                                                                                                                                  |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Management FQDN</b>     | The FQDN to assign to the System Manager application.<br><br>* <b>Note:</b><br>System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager. |
| <b>IPv6 Address</b>        | The IPv6 address of the System Manager application for out of band management. The field is optional.                                                                                        |
| <b>IPv6 Network prefix</b> | The IPv6 subnetwork mask to assign to the System Manager application. The field is optional.                                                                                                 |
| <b>IPv6 Gateway</b>        | The gateway IPv6 address to assign to the System Manager application. The field is optional.                                                                                                 |
| <b>Default Search List</b> | The search list of domain names. The field is optional.                                                                                                                                      |
| <b>NTP Server IP/FQDN</b>  | The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).                                                                                  |
| <b>Time Zone</b>           | The timezone where the System Manager application is located. A list is available where you select the name of the continent and the name of the country.                                    |

## Public Network Settings

| Name                              | Description                                                                                  |
|-----------------------------------|----------------------------------------------------------------------------------------------|
| <b>Public IP Address</b>          | The IPv4 address to enable public access to different interfaces. The field is optional.     |
| <b>Public Netmask</b>             | The IPv4 subnetwork mask to assign to System Manager application. The field is optional.     |
| <b>Public Gateway</b>             | The gateway IPv4 address to assign to the System Manager application. The field is optional. |
| <b>Public FQDN</b>                | The FQDN to assign to the System Manager application. The field is optional.                 |
| <b>Public IPv6 Address</b>        | The IPv6 address to enable public access to different interfaces. The field is optional.     |
| <b>Public IPv6 Network Prefix</b> | The IPv6 subnetwork mask to assign to System Manager application. The field is optional.     |
| <b>Public IPv6 Gateway</b>        | The gateway IPv6 address to assign to the System Manager application. The field is optional. |



## Virtual FQDN

| Name             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Hostname | <p>The virtual hostname of the System Manager application.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.</li> <li>• VFQDN is a mandatory field.</li> <li>• By default, VFQDN entry gets added in the <code>/etc/hosts</code> file during installation. Do not remove VFQDN entry from the <code>/etc/hosts</code> file.</li> <li>• VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value.</li> <li>• You must keep VFQDN domain value same as of FQDN domain value.</li> <li>• If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved.</li> <li>• Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address.</li> <li>• In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.</li> <li>• After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:             <ol style="list-style-type: none"> <li>1. Log in to System Manager with administrator privilege credentials.</li> <li>2. Run the <b>changeVFQDN</b> command.</li> </ol> </li> </ul> <p> <b>Important:</b></p> <p>When you run the <b>changeVFQDN</b> command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.</p> |
| Virtual Domain   | The virtual domain name of the System Manager application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Name                    | Description                 |
|-------------------------|-----------------------------|
| SNMPv3 User Name Prefix | The prefix for SNMPv3 user. |

*Table continues...*

| Name                                                | Description                                                                      |
|-----------------------------------------------------|----------------------------------------------------------------------------------|
| <b>SNMPv3 User Authentication Protocol Password</b> | The password for SNMPv3 user authentication.                                     |
| <b>Confirm Password</b>                             | The password that you retype to confirm the SNMPv3 user authentication protocol. |
| <b>SNMPv3 User Privacy Protocol Password</b>        | The password for SNMPv3 user privacy.                                            |
| <b>Confirm Password</b>                             | The password that you must provide to confirm the SNMPv3 user privacy protocol.  |

## SMGR CLI USER

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SMGR command line user name</b>     | <p>The user name of the System Manager CLI user.</p> <p> <b>Note:</b></p> <p>Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcasa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.</p> |
| <b>SMGR command line user password</b> | The password for the System Manager CLI user.                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Confirm Password</b>                | The password that you retype to confirm the System Manager CLI user authentication.                                                                                                                                                                                                                                                                                                                                  |

## Backup Definition

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schedule Backup?</b>             | <ul style="list-style-type: none"> <li>• <b>Yes:</b> To schedule the backup jobs during the System Manager installation.</li> <li>• <b>No:</b> To schedule the backup jobs later.</li> </ul> <p> <b>Note:</b></p> <p>If you select <b>No</b>, the system does not display the remaining fields.</p> |
| <b>Backup Server IP</b>             | <p>The IP address of the remote backup server.</p> <p> <b>Note:</b></p> <p>The IP address of the backup server must be different from the System Manager IP address.</p>                                                                                                                            |
| <b>Backup Server Login Id</b>       | The login ID of the backup server to log in through the command line interface.                                                                                                                                                                                                                                                                                                        |
| <b>Backup Server Login Password</b> | The SSH login password to log in to the backup server from System Manager through the command line interface.                                                                                                                                                                                                                                                                          |

*Table continues...*

| Name                             | Description                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Confirm Password</b>          | The password that you reenter to log in to the backup server through the command line interface.                                                                  |
| <b>Backup Directory Location</b> | The location on the remote backup server.                                                                                                                         |
| <b>File Transfer Protocol</b>    | The protocol that you can use to create the backup. The values are SCP and SFTP.                                                                                  |
| <b>Repeat Type</b>               | The type of the backup. The possible values are: <ul style="list-style-type: none"> <li>• Hourly</li> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> </ul> |
| <b>Backup Frequency</b>          | The frequency of the backup taken for the selected backup type.<br>The system generates an alarm if you do not schedule a System Manager backup every seven days. |
| <b>Backup Start Year</b>         | The year in which the backup must start. The value must be greater than or equal to the current year.                                                             |
| <b>Backup Start Month</b>        | The month in which the backup must start. The value must be greater than or equal to the current month.                                                           |
| <b>Backup Start Day</b>          | The day on which the backup must start. The value must be greater than or equal to the current day.                                                               |
| <b>Backup Start Hour</b>         | The hour in which the backup must start.<br>The value must be six hours later than the current hour.                                                              |
| <b>Backup Start Minutes</b>      | The minute when the backup must start. The value must be a valid minute.                                                                                          |
| <b>Backup Start Seconds</b>      | The second when the backup must start. The value must be a valid second.                                                                                          |

### Enhanced Access Security Gateway (EASG) - EASG User Access

| Name                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG</b> | <p>Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• 1: To enable EASG.</li> <li>• 2: To disable EASG.</li> </ul> <p>Avaya recommends to enable EASG.</p> <p>You can also enable EASG after deploying or upgrading the application by using the command: <b>EASGManage --enableEASG</b>.</p> |

## Customer Root Account

### \* Note:

The **Customer Root Account** field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the **Customer Root Account** field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

| Name                                                     | Description                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Customer Root Account for this Application</b> | Enables or disables the customer root account for the application.<br><br>Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click <b>Accept</b> .<br><br>When you accept the root access statement, the system displays the <b>Customer Root Password</b> and <b>Re-enter Customer Root Password</b> fields. |
| <b>Customer Root Password</b>                            | The root password for the application                                                                                                                                                                                                                                                                                                       |
| <b>Re-enter Customer Root Password</b>                   | The root password for the application                                                                                                                                                                                                                                                                                                       |

## Data Encryption

### \* Note:

- From Release 8.1.2 and later, Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment.
- For data encryption, you must use a new encryption capable variant of Release 8.1E OVA.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.

| Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Encryption</b>                 | <p>Enables or disables the data encryption.</p> <p>The options are:</p> <ul style="list-style-type: none"> <li>• <b>1:</b> To enable the data encryption.</li> <li>• <b>2:</b> To disable the data encryption.</li> </ul> <p> <b>Important:</b></p> <ul style="list-style-type: none"> <li>• An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa.</li> <li>• While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled.</li> <li>• <b>On Solution Deployment Manager:</b> When the <b>Data Encryption</b> field is set to 1, the system enables the <b>Encryption Pass-Phrase</b> and <b>Re-enter Encryption Pass-Phrase</b> fields to enter the encryption passphrase.</li> <li>• <b>On vCenter or ESXi:</b> When the <b>Data Encryption</b> field is set to 1, enter the encryption passphrase in the <b>Password</b> and <b>Confirm Password</b> fields.</li> </ul> |
| <b>Encryption Pass-Phrase</b>          | <p>This field is applicable when data encryption is enabled.</p> <p>The passphrase for data encryption.</p> <p>When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules.</p> <p>When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Re-enter Encryption Pass-Phrase</b> | <p>The passphrase for data encryption.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Require Encryption Pass-Phrase at Boot-Time</b> | <p>If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default, the <b>Require Encryption Pass-Phrase at Boot-Time</b> check box is selected.</p> <p> <b>Important:</b></p> <p>You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application.</p> <p>If you lose the data encryption passphrase, the only option is to reinstall the OVA.</p> <p>If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure.</p> <p>You can also set up the remote key server by using the <b>encryptionRemoteKey</b> command after the deployment of the application.</p> |

## Network Parameters

| Name                                     | Description                                                                                           |
|------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Out of Band Management IP Address</b> | The IP Address that you must assign to the Out of Band Management port group. The field is mandatory. |
| <b>Public</b>                            | The port number that you must assign to public port group. The field is optional.                     |

| Button         | Description                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------|
| <b>Upgrade</b> | Displays the EULA acceptance screen. To accept EULA and start the upgrade process, click <b>Accept</b> . |

---

## Upgrade job status

---

### Upgrade job status

The Upgrade Job Status page displays the status of completion of every upgrade job that you performed. Every step that you perform to upgrade an application by using Solution Deployment Manager is an upgrade job.

You must complete the following jobs to complete the upgrade:

1. **Refresh Element(s):** To get the latest data like version data for the applications in the system.

2. **Analyze:** To evaluate an application that completed the Refresh Element(s) job.
3. **Pre-Upgrade Check:** To evaluate an application that completed the Analyze job.
4. **Upgrade:** To upgrade applications that completed the Pre-upgrade Check job.
5. **Commit:** To view commit jobs.
6. **Rollback:** To view rollback jobs.
7. **Uninstall:** To view uninstall jobs.

---

## Viewing the Upgrade job status

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Status of Upgrade Management Jobs page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **View**.

The system displays the Upgrade Job Status page.

---

## Editing an upgrade job

### Before you begin

You can edit the configuration of an upgrade job that is in pending state.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click **Upgrade**.
4. Select a pending upgrade job that you want to edit.
5. Click **Edit Configuration**.

The system displays the Upgrade Configuration page.

6. To edit the configuration, see Upgrading Avaya Aura applications.

---

## Deleting the Upgrade jobs

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.

2. In the left navigation pane, click **Upgrade Job Status**.
3. On the Upgrade Job Status page, in the **Job Type** field, click a job type.
4. Select one or more jobs.
5. Click **Delete**.

The system updates the Upgrade Job Status page.

## Upgrade Job Status field descriptions

| Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Job Type</b>           | The upgrade job type. The options are: <ul style="list-style-type: none"> <li>• <b>Refresh Element(s)</b>: To view refresh elements jobs.</li> <li>• <b>Analyze</b>: To view analyze jobs.</li> <li>• <b>Pre-Upgrade Check</b>: To view preupgrade check jobs.</li> <li>• <b>Upgrade</b>: To view upgrade jobs.</li> <li>• <b>Commit</b>: To view commit jobs.</li> <li>• <b>Rollback</b>: To view rollback jobs.</li> <li>• <b>Uninstall</b>: To view uninstall jobs.</li> </ul> |
| <b>Job Name</b>           | The upgrade job name.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Start Time</b>         | The time when the system started the job.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>End Time</b>           | The time when the system ended the job.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Status</b>             | The status of the upgrade job. The status can be: SUCCESSFUL, PENDING_EXECUTION, PARTIAL_FAILURE, FAILED.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>% Complete</b>         | The percentage of completion of the upgrade job.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Element Records</b>    | The total number of elements in the upgrade job.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Successful Records</b> | The total number of times that the upgrade job ran successfully.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Failed Records</b>     | The total number of times that the upgrade job failed.                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Button                    | Description                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------|
| <b>Delete</b>             | Deletes the upgrade job.                                                                        |
| <b>Re-run Checks</b>      | Performs the upgrade job again.                                                                 |
| <b>Edit Configuration</b> | Displays the Upgrade Configuration page where you can change the upgrade configuration details. |



---

# Upgrades to Communication Manager Release 6.3.100

---

## Communication Manager upgrades

System Manager provides the user interface to upgrade Communication Manager and the associated devices to Release 6.3.100. However, you must select the target release 6.3.8 from **Solution Deployment Manager > Upgrade Release Selection**.

The Software Inventory page in Upgrade Management consists of a collective inventory of different devices arranged in a hierarchy.

When you select more than one element in a hierarchy, the system creates a scheduler job for the upgrade. Each hierarchy can have only one job scheduled. The system determines the sequence in which the elements must be upgraded. The devices might include:

- Communication Manager
- Communication Manager Messaging
- Utility Server
- Branch Session Manager
- Gateways
- TN Boards
- Media modules

If one of the devices fails to upgrade within the hierarchy, the system might proceed or process the job as failed based on the compatibility of the failed device with the subsequent device.

### Important:

You cannot select Communication Manager Release 5.2.1 and Avaya Virtualization Platform-based Communication Manager Release 6.x together. You can only upgrade Communication Manager Release 5.2.1 systems together or all Appliance Virtualization Platform-based Communication Manager Release 6.x systems at a time.

You can perform the following operations by using the **Upgrade Management > Software Inventory**:

- Get Inventory
- Analyze software
- Download
- Perform a preupgrade check
- Reset or backup Communication Manager
- Sequence upgrades
- Upgrade the following:
  - System Platform-based Communication Manager Release 6.x to Release 6.3.100
  - Linux-based Communication Manager Release 5.x to Release 5.2.1

**★ Note:**

Install System Platform on the supported server before you upgrade Communication Manager

- All devices and components that run on Communication Manager
- Commit, rollback, or cancel the template upgrade
- Update Communication Manager, SAMP firmware, and MPC firmware
- Upgrade gateways, TN boards, and media modules

### Guidelines for upgrading Communication Manager and Messaging elements

1. Before upgrading the Communication Manager and Messaging elements to major Release 6.3.x and later, note down the Communication Manager and Messaging templates associated with user provisioning rule in System Manager.
2. Once the Communication Manager or Messaging element is upgraded, then templates associated with old release of Communication Manager and Messaging will get unlinked for existing user provisioning rule. Therefore, after upgrading Communication Manager and Messaging elements:
  - a. Create custom templates for the current release of Communication Manager and Messaging.
  - b. Update existing user provisioning rule with newly created custom templates or default templates of Communication Manager and Messaging as per the user provisioning rule guidelines.

## Checklist for upgrading Communication Manager to Release 6.3.100

### Performing the initial setup

| Task                                                                                                                                                                                                                                           | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Install the physical or virtual servers that support the Avaya Aura® applications that you want to deploy.</li> <li>2. Deploy System Manager, Communication Manager, and Session Manager.</li> </ol> | <p>You require the working knowledge of the following Avaya Aura® applications: Communication Manager, System Manager, Session Manager, and Branch Session Manager.</p> <p>You require the working knowledge of the following processes:</p> <ul style="list-style-type: none"> <li>• Setting up PLDS.</li> <li>• Downloading Avaya Aura® applications from PLDS</li> <li>• Configuring a standalone FTP, SCP, HTTP, or SFTP server to host Avaya Aura® applications.</li> </ul> <p>You require the administrator credentials for the Avaya Aura® applications that you are upgrading.</p> |

## Performing the preconfiguration steps

| Task                                                                                                                                                                                                    | Notes                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Click <b>Save Trans</b> to save the changes that you have made.                                                                                                                                         |                                                                                 |
| Ensure that you have sufficient disk space for the server that you have attached with the software library.                                                                                             |                                                                                 |
| Create a user with administrator credentials to gain access for the elements using HTTP, FTP, SCP or SFTP services.                                                                                     | <a href="#">Protocol requirements to configure a remote server</a> on page 1294 |
| For the Communication Manager instance that you have created, create a user and user profile.                                                                                                           | <a href="#">Creating a new user account</a> on page 225                         |
| Configure SNMP for the user.                                                                                                                                                                            | <a href="#">Creating an SNMPv3 user profile</a> on page 956                     |
| Create the EPW file for the Communication Manager instance by using the following templates: <ul style="list-style-type: none"> <li>• Embedded CM Main</li> <li>• Embedded Survivable Remote</li> </ul> |                                                                                 |
| Add the following files: <ol style="list-style-type: none"> <li>1. System Platform authentication file</li> <li>2. Communication Manager 6.x license file</li> </ol>                                    |                                                                                 |
| Ensure that you have the PLDS access credentials and Company ID.                                                                                                                                        |                                                                                 |
| Administer Branch Session Manager in System Manager.                                                                                                                                                    |                                                                                 |

## Managing elements inventory

| Task                                                                | Notes                                                                            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Configure Communication Manager for administration and SNMP access. | <a href="#">Creating an SNMP target profile</a> on page 960                      |
| Configure the access to the H.248 gateway device.                   | <a href="#">Adding G430 or G450 Branch Gateway to System Manager</a> on page 928 |

## Performing the software management configuration settings

| Task                                                                                                                               | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Option 1: Set up PLDS access through the Avaya Support site at <a href="https://support.avaya.com">https://support.avaya.com</a> . | <p>Log in to the PLDS website at <a href="http://plds.avaya.com">http://plds.avaya.com</a>.</p> <p>Use your PLDS account to get your Company ID.</p> <p>On the System Manager web console, go to <b>Services &gt; Solution Deployment Manager &gt; User Settings</b>.</p> <p>Enter the following details to get entitlements for analyze and artifacts for download:</p> <ol style="list-style-type: none"> <li>1. SSO user name</li> <li>2. SSO password</li> <li>3. Company ID</li> </ol> |
| Option 2: Set up the PLDS access through an alternate source.                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Set up the software library.                                                                                                       | <a href="#">Creating a software library</a> on page 1303                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Performing the upgrade process

| Task                                                                                            | Notes                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Collect the software inventory.                                                                 | Perform the Get Inventory operation when you modify the PLDS access or alternate source. For more information, see <a href="#">Software inventory</a> on page 1439                                                                                                                                                                                                                                  |
| Perform the Analyze Software operation for the Communication Manager element that you selected. | <a href="#">Analyzing the software</a> on page 1445                                                                                                                                                                                                                                                                                                                                                 |
| Download the software.                                                                          | <a href="#">Downloading the software</a> on page 1445                                                                                                                                                                                                                                                                                                                                               |
| Run the preupgrade check for the selected Communication Manager device.                         | <a href="#">Performing a preupgrade check</a> on page 1446                                                                                                                                                                                                                                                                                                                                          |
| Run the upgrade operation.                                                                      | <p><a href="#">Upgrading a Communication Manager</a> on page 1484</p> <p><a href="#">Upgrading a Communication Manager Release 5x</a> on page 1472</p> <p><a href="#">Upgrading communication manager 6x</a> on page 1453</p> <p> <b>Note:</b></p> <p>The upgrade process takes about 2.5 hours to complete.</p> |

## Installing the service packs

| Task                                                                      | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installing the service pack or software patches on Communication Manager. | <a href="#">Updating Communication Manager</a> on page 1485                                                                                                                                                                                                                                                                                                                                                                            |
| Updating the <b>H.248 Media Gateway</b> device.                           | <ol style="list-style-type: none"> <li>1. In the alternate source location, download the patch file <code>g450_sw_36_9_0.bin</code>.</li> <li>2. For the gateway that you have selected, perform the Analyze job.</li> <li>3. On the Select Gateway (G) panel, select <b>Library and download protocol</b>.</li> <li>4. Click <b>Download</b>.</li> <li>5. Click the active status link to observe the progress of upgrade.</li> </ol> |

## Getting inventory

### About this task

Before you perform any operation on Communication Manager 6.3.x or earlier, perform the get inventory operation to ensure that the system reflects the exact state of the device in Software Inventory.

Do not perform the following during an upgrade:

- The get inventory operation when the upgrade is in progress.
- The analyze operation when the upgrade is in progress.
- The analyze operation during the get inventory operation.
- Log on the Dom0, Cdom, or virtual machine.

### Before you begin

- Configure the SNMP parameters on the device before you configure the same device in System Manager from Manage Elements.

#### **Note:**

Use the same SNMP credentials for the device in System Manager.

- To upgrade a Communication Manager device, you must configure a profile 18 user on Communication Manager. You cannot use init and craft user profiles while configuring a profile 18 user.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.

4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the device or devices for which you want to obtain the inventory, and perform the following:
  - To get the inventory now, click **Get Inventory > Now**.
  - To get the inventory later, click **Get Inventory > Schedule**.

 **Note:**

If you click **Get Inventory**, the system automatically analyzes the devices. You need not analyze the devices again.

## Analyze software

The analyze software operation finds and displays the latest release of a device in the **Available Software** column. This operation changes the icon in the **State** column after comparing the current software version of the device with the latest version. To get the latest version, use **Get Inventory**.

 **Note:**

| Icon                                                                                | State           | Description                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Unknown         | Indicates that the device is yet to be analyzed.                                                                                                                                                |
|  | Update Required | Indicates that a new version of the software is available and the device must be upgraded. Also indicates that the software file is not downloaded to the System Manager software file library. |
|  | Ready to Update | Indicates that an upgrade is required for the device and the new version of the software is downloaded to the software file library. Also indicates that the device is ready for upgrade. .     |
|  | Updated         | Indicates that the device is on the latest version.                                                                                                                                             |
|  | Non Upgradable  | Indicates that you cannot upgrade the component, and the component is only listed as part of the inventory.                                                                                     |
|  | Unentitled      | Indicates that the new version of the software is available, but you are not entitled to the new version.                                                                                       |

---

## Analyzing the software

### About this task

Using the analyze feature, you can identify whether a new software is available for the inventory that you collected, and whether you have permissions to download the software.

### Before you begin

- Get the inventory. If multiple sites work on the same survivable remote server, get the inventory before you perform the analyze operation.
- Configure user settings.
- Ensure that the inventory is populated.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select one or more devices, and perform one of the following:
  - To analyze all devices, click **Analyze > Analyze All Now**.
  - To analyze all devices at a later time, click **Analyze > Analyze All Scheduled**.
  - To analyze selected devices, click **Analyze > Analyze Selected Now**.
  - To analyze selected devices at a later time, click **Analyze > Analyze Selected Scheduled**.

---

## Downloading the software

### Before you begin

- Analyze the software.
- Create a software library.
- Ensure that 9 GB disk space is available on System Manager.

To view the available disk space, log in to the System Manager command line interface, and type `df -h /opt/Avaya/`.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.

3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the devices, and click **Download**.

The system displays the File Download Manager page.

6. For Branch Session Manager, perform the following:
  - a. In the **Select Software/Hardware Types** section, select Branch Session Manager and click **Show files**.
  - b. Select `asm-patch-6.3.2.1.632006.sh`.
7. In the **Select Files Download Details** section, select **Source** and the files that you want to download.

 **Note:**

Do not select the redundant `6.3.0.0.1105.iso` file.

Based on the type of the software or hardware, select the required `6.3.0.0.1105.iso` file.

8. Click **Download**.

The system displays the Files Download Manager — Library and Protocol Selection page.

9. Select the **Library** and **Protocol**, and click **Download**.
10. On the End User Licensing Agreement page, read the License Agreement, and if you agree to its terms, click **I Agree to the above end user license agreement** and do one of the following:
  - Click **Now** to begin the download immediately.
  - Click **Schedule** to schedule the download for a later time.

The system displays the Files Download Manager page, where the **File Download Status** section displays the download details.

## Result

After you download the recommended files, on the Software Inventory page the state of the device changes to  that is “ready to update”.

---

## Performing a preupgrade check

### Before you begin

#### For Communication Manager 5.2.1:

- Create the authorization file for System Platform, and store the file in a local folder.
- For more information, contact Avaya support team.



- Create the new EPW file for the Communication Manager to be upgraded, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server.

For more information, contact Avaya support team.

- Get the WebLM server IP address for licensing.

For more information contact the Avaya support team.

- Get the inventory for Communication Manager 5.2.1.
- Analyze the software.
- Download the related firmware for Communication Manager 5.2.1 upgrade.

#### For Communication Manager 6.x:

- Get the inventory.
- Analyze the software.
- Download the related firmware for the Communication Manager upgrade.
- Run the preupgrade check for the supported servers, compatible template, and the memory requirement in System Manager.

For more information, see Hardware requirement checks during preupgrade check.

#### About this task

Install the latest System Platform on the server. You can stop the preupgrade check for elements that are in queue.

#### Note:

- System Platform must be on the same subnetwork as Communication Manager 5.2.1.
- During preupgrade, if the mandatory check fails, the **Upgrade** button becomes unavailable.
- If you fail to perform preupgrade, the **Upgrade**, **Commit**, **Rollback**, **Cancel Template Upgrade**, **Backup CM/CMM**, and **More Actions** buttons become unavailable.
- You can select about four templates to perform the preupgrade check.

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the templates that you want to upgrade.  
You can select only templates.
6. Click **Pre-Upgrade Check**.

The system displays the status with the icons. For more information, see Preupgrade status.

7. To run the preupgrade check for templates again, on the Pre-upgrade Check Running Status page, select one or more templates and click **Run**.
8. **(Optional)** To stop the committed preupgrade check for the template, click **Cancel**.
9. On the Software Inventory page, view the status of the preupgrade check for an element in the **Pre-Upgrade Check Status** column.

#### Related links

[Preupgrade status](#) on page 1451

[Preupgrade checks](#) on page 1448

---

## Preupgrade checks

**The system runs the following preupgrade checks for Communication Manager 5.2.1:**

- Mandatory checks:
  - Hardware compatibility check
  - Required files download check
- Recommended check:
  - Sufficient memory check

**The system runs the following preupgrade checks for System Platform-based Communication Manager 6.x:**

- Mandatory checks:
  - RAID battery check
  - Hardware compatibility check
  - Required files download check
  - CDOM credentials check
  - Disk space check
- Recommended check:
  - Sufficient memory check
  - Version compatibility check
  - Bandwidth is sufficient check
- Informational check:
  - Sufficient memory check

#### **Note:**

Do not perform any jboss operations while upgrade is in progress.

## Preupgrade checklist for Linux® Operating System upgrades

Perform the following checks before you start upgrading elements that you have deployed on System Manager on Linux® Operating System to System Manager on Appliance Virtualization Platform, on the same server or a different server:

 **Note:**

| No. | Task                                                                                                                                            | ✓ |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Ensure that you assign a different IP address for the ESXi host                                                                                 |   |
| 2   | After you perform the <b>Refresh Element(s)</b> operation, ensure that your system contains the latest version of all elements.                 |   |
| 3   | On the User Settings page, ensure that PLDS or the alternate source are configured correctly.                                                   |   |
| 4   | After you perform the <b>Analyze</b> operation, verify on the Upgrade Job status page that the operation you performed is successful.           |   |
| 5   | Download the OVA file for the element that you want to upgrade.                                                                                 |   |
| 6   | After you have performed the <b>Analyze</b> job, verify that the element that you want to upgrade displays the <b>Ready for Upgrade</b> status. |   |
| 7   | On the Pre-upgrade Check Job Details page, ensure that the status of the element that you want to upgrade displays <b>Successful</b> .          |   |
| 8   | In the <b>Upgrade Job</b> status, in the Pre-upgrade Configuration page, verify the configuration values are correct.                           |   |

## Pre-upgrade checklist for System Platform upgrades

Perform the following checks before you start upgrading elements on System Manager that you have deployed on System Platform to System Manager on System Platform, on the same server or a different server:

 **Note:**

| No. | Task                                                                                                                                                                                                                                                                                                                                                                                 | ✓ |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1   | Ensure that you assign a different IP address for the ESXi host.                                                                                                                                                                                                                                                                                                                     |   |
| 2   | Ensure that you have added all the elements on the System Platform and you have established a structural relationship among all those elements. Elements include Communication Manager Utility Server, CDOM, System Platform and the Communication Manager itself that will be upgraded to Avaya Aura® Virtualized Appliance or VMware in customer-provided Virtualized Environment. |   |

*Table continues...*

| No. | Task                                                                                                                                            | ✓ |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 3   | After you perform the <b>Refresh Element(s)</b> operation, ensure that your system contains the current version of all the elements.            |   |
| 4   | On the User Settings page, ensure that the PLDS or the Alternate source are configured correctly.                                               |   |
| 5   | After you perform the <b>Analyze</b> operation, verify on the Upgrade Job Status page that the operation that you performed is successful.      |   |
| 6   | Download the OVA file for the element that you want to upgrade.                                                                                 |   |
| 7   | After you have performed the <b>Analyze</b> job, verify that the element that you want to upgrade displays the <b>Ready for Upgrade</b> status. |   |
| 8   | On the Pre-upgrade Check Job Details page, ensure that the element that you want to upgrade displays status as <b>Successful</b> .              |   |
| 9   | In the <b>Upgrade Job Status</b> section, on the Pre-upgrade Configuration page, verify the configuration values are correct.                   |   |

## Hardware requirement checks during a preupgrade check

During the preupgrade check, the system checks the supported servers, template compatibility, and memory requirement in System Manager.

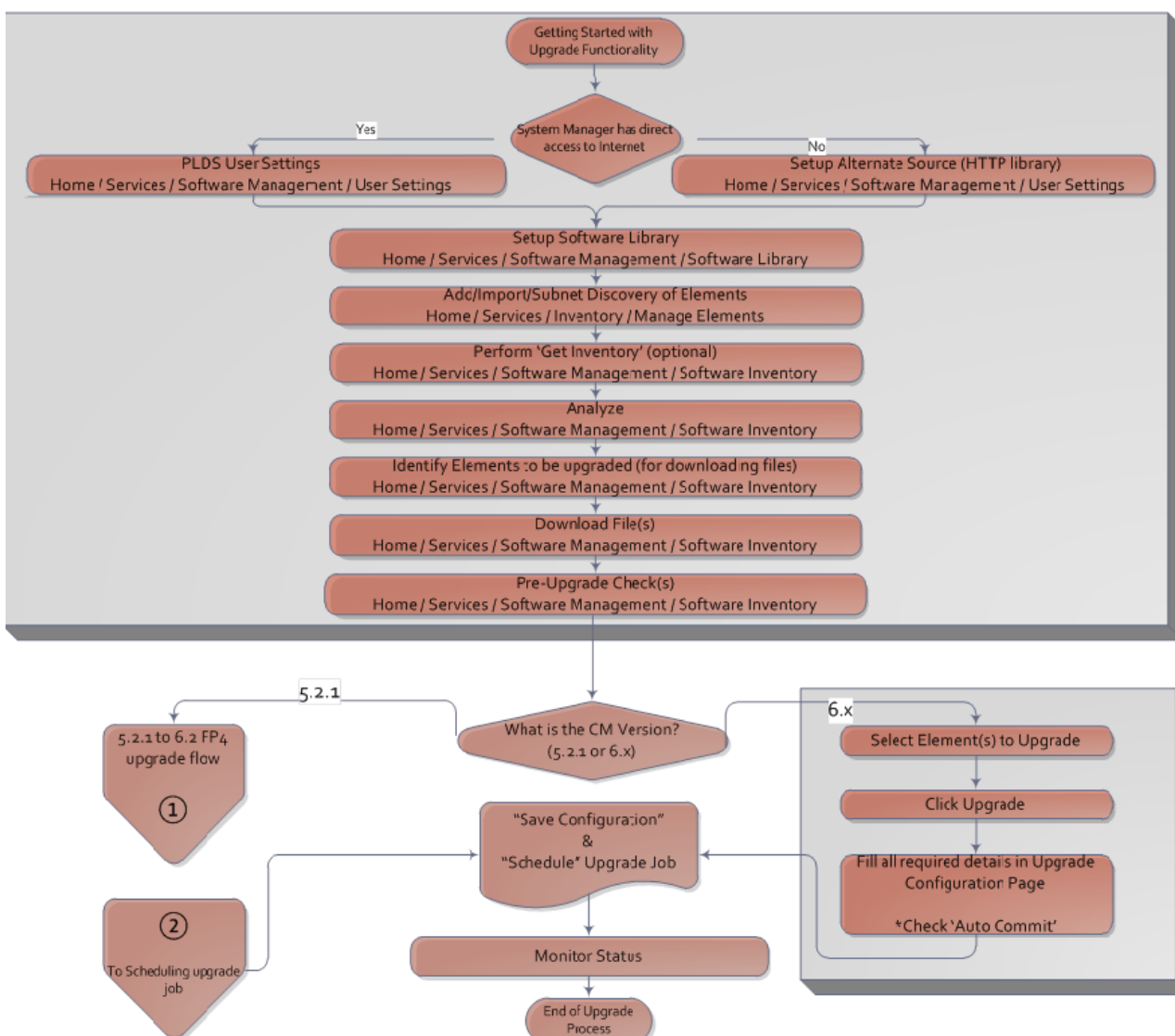
| Template           | Server type                                                                                                                                                                            | Minimum memory requirement |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| CM_Duplex          | Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360p G8, and HP ProLiant DL360 G9<br><br>Avaya Solutions Platform 120 Appliance and Avaya Solutions Platform 130 Appliance | 12 GB                      |
| CM_Simplex         | Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360p G8, and HP ProLiant DL360 G9<br><br>Avaya Solutions Platform 120 Appliance and Avaya Solutions Platform 130 Appliance | 8 GB                       |
| CM_SurvRemote      | Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360p G8, and HP ProLiant DL360 G9<br><br>Avaya Solutions Platform 120 Appliance and Avaya Solutions Platform 130 Appliance | 8 GB                       |
| CM_SurvRemoteEmbed | S8300E                                                                                                                                                                                 | 8 GB                       |
| CM_onlyEmbed       | S8300E                                                                                                                                                                                 | 8 GB                       |

## Preupgrade status

| Icon                                                                              | State                                  | Description                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Unknown or Not-Started                 | Indicates that the preupgrade check has not started, or was not run earlier.                                                                                                                |
|  | Failed                                 | Indicates that one or more mandatory preupgrade checks failed, and the failed elements are unavailable for upgrade as the probability of upgrade failure is high.                           |
|  | Success with recommended check failure | Indicates that mandatory preupgrade checks are successful, but one or more recommended checks failed. The elements are available for upgrade as the probability of upgrade failure is less. |
|  | Successful                             | Indicates that all preupgrade checks are successful, and the probability of successful upgrade is high.                                                                                     |

## Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3

### Communication Manager upgrade workflow Procedure



## Related links

[Analyze software](#) on page 1444

[CM Upgrade Configuration field descriptions](#) on page 1466

[Analyzing the software](#) on page 1445

[Performing a preupgrade check](#) on page 1446

[Preupgrade checks](#) on page 1448

[System Platform Templates Upgrade Configuration field descriptions](#) on page 1458

[Software Inventory field descriptions](#) on page 1460

[Device list](#) on page 901

## Communication Manager 6.x upgrade checklist

For upgrades to Communication Manager 6.3.100, customer must reconfigure the SNMP alarming on the upgraded system.

| No. | Task                                                                                                                 | References                                                                               | ✓ |
|-----|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|---|
| 1.  | Install System Platform and the required patch on the supported server.                                              | —                                                                                        |   |
| 2.  | Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page. | <a href="#">Creating discovery profiles and discovering elements</a> on page 899         |   |
| 3.  | Configure user settings.                                                                                             | <a href="#">Establishing PLDS connection to Avaya</a> on page 1287                       |   |
| 4.  | Create a remote software library.                                                                                    | <a href="#">Creating a software library</a> on page 1303                                 |   |
| 5.  | Get the inventory for Communication Manager 6.x.                                                                     | <a href="#">Getting inventory</a> on page 1443                                           |   |
| 6.  | Analyze the software.                                                                                                | <a href="#">Analyzing the software</a> on page 1445                                      |   |
| 7.  | Download the related firmware for the Communication Manager upgrade.                                                 | <a href="#">Downloading the software</a> on page 1445                                    |   |
| 8.  | Run the preupgrade check.                                                                                            | <a href="#">Performing a preupgrade check</a> on page 1446                               |   |
| 9.  | Perform the upgrade.                                                                                                 | <a href="#">Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.100</a> on page 1453 |   |
| 10. | Verify that the upgrade is successful.                                                                               | <a href="#">Verifying the upgrade</a> on page 1455.                                      |   |

### Related links

[Device list](#) on page 901

## Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.100

### About this task

Use the procedure to upgrade Communication Manager 6.0, 6.1, or 6.2 that is running on System Platform to Release 6.3.100.

For the supported upgrade paths of System Platform, see *Upgrading Avaya Aura® System Platform*.

### ! Important:

For duplex system, first upgrade the standby Communication Manager. When the standby Communication Manager upgrade is complete, upgrade the active Communication Manager.

For more information about postupgrade steps for duplex templates, see *Upgrading Avaya Aura® Communication Manager*.

When you upgrade a System Platform-based Communication Manager with:

- Branch Session Manager, the system upgrades Branch Session Manager
- Communication Manager Messaging, the system upgrades Communication Manager Messaging

### Before you begin

- Get the inventory.
- Analyze the software.
- Download the software.
- Run the preupgrade check.
- Run the hardware requirement checks during the preupgrade check.

During the preupgrade check, the system checks the supported servers, template compatibility, and the memory requirement in System Manager.

For more information, see Hardware requirement checks during a preupgrade check.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the templates that you want to upgrade.
6. Click **Upgrade**.
7. On the System Platform Template(s) Upgrade Configuration page, select one or more templates of the same type.
8. In the **Upgrade Configuration** section, select the templates that you want to upgrade and complete the fields.

For more information, see System Platform Template(s) Upgrade Configuration field descriptions.

9. Perform one of the following actions:

- To upgrade the solution template automatically, select **Auto Commit Upgrade**.

#### **Important:**

You cannot perform rollback if you select **Auto Commit Upgrade**.

- To commit the upgrade of the Communication Manager template manually, perform the following:
  - a. Clear the **Auto Commit Upgrade** check box.
  - b. On the Software Inventory page, click **More Actions > Commit Template Upgrade**.



10. **(Optional)** If you find any errors or issues, click **More Actions > Rollback Template Upgrade**.

The system rolls back the software to the original version.

11. **(Optional)** To stop the upgrade during template installation, click **More Actions > Cancel Template Upgrade**.
12. Click **Save the configuration**.
  - To cancel the operation, click **Clear configuration**.
13. In the **Job Schedule** section, perform one of the following:
  - To upgrade the device, click **Now**.
  - To upgrade the device at a later time, click **Later**.
14. Click **Upgrade**.

### Next steps

Verify that the upgrade is successful.

For more information, see “Verifying the upgrade”.

### Related links

[Analyze software](#) on page 1444

[Analyzing the software](#) on page 1445

[Performing a preupgrade check](#) on page 1446

[Preupgrade checks](#) on page 1448

[Device list](#) on page 901

## Verifying the upgrade

### Before you begin

Complete the upgrade of Communication Manager and devices.

### About this task

#### Important:

For more information about postupgrade steps for a duplex template, see *Upgrading Avaya Aura® Communication Manager*.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, click the status of the Communication Manager device to view the logs and the description of the upgrade operation.

The system displays the status of the upgrade in **Status** column.

6. To verify that the upgrade is successful, check the following on the Software Inventory page:
  - The **Release** column displays the updated icon .
  - The **Update** column displays the updated icon .
  - The **Sw Release** changed from the previous release to the latest upgraded release.
  - The **Status** changed from **Upgrade Scheduled** to **IDLE**.
7. Validate that the Communication Manager 5.2.1 server data that is restored on Release 7.1.1. If the server data on the Release 7.1.1 system is incomplete, complete the required fields.

 **Important:**

This validation applies only to Communication Manager Release 5.2.1.

For more information about the following, see *Upgrading Avaya Aura® Communication Manager*:

- Recording the configuration screens.
- Worksheet for upgrading Communication Manager to simplex and embedded templates.

## Sample scenario to upgrade Communication Manager Release 6.x to 6.3.100

To upgrade Communication Manager Release 6.x to 6.3.100, do the following:

1. Perform the [Preupgrade tasks](#) on page 1456
2. Perform the [Upgrading Communication Manager 6.x to 6.3.100](#) on page 1457
3. Perform [Verifying the upgrade](#) on page 1455

### Preupgrade tasks

| No. | Task                                                                                                                 | References                                                    |  |
|-----|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 1.  | Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page. | <a href="#">Discovering elements</a> on page 899              |                                                                                       |
| 2.  | Configure user settings.                                                                                             | <a href="#">Configuring user settings</a> on page 1287        |                                                                                       |
| 3.  | Create a remote software library.                                                                                    | <a href="#">Creating a software library</a> on page 1303      |                                                                                       |
| 4.  | Get the inventory for Communication Manager 6.x.                                                                     | <a href="#">Get inventory software inventory</a> on page 1443 |                                                                                       |

*Table continues...*

| No. | Task                                                                 | References                                                                   | ✓ |
|-----|----------------------------------------------------------------------|------------------------------------------------------------------------------|---|
| 5.  | Analyze the software.                                                | <a href="#">Analyzing the software for software inventory</a> on page 1445   |   |
| 6.  | Download the related firmware for the Communication Manager upgrade. | <a href="#">Downloading the software for software inventory</a> on page 1445 |   |
| 7.  | Run the preupgrade check.                                            | <a href="#">Performing the preupgrade check</a> on page 1446                 |   |

## Upgrading Communication Manager 6.x to 6.3.100

### Before you begin

Complete the preupgrade tasks.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 6.x device that you want to upgrade.
6. Click **Upgrade**.
7. On the System Platform Template(s) Upgrade Configuration page, select **CM\_Simplex**.
8. In the **Upgrade Configuration** section, select one or more templates that you want to upgrade and complete the fields.  
  
For more information, see System Platform Template(s) Upgrade Configuration field descriptions.
9. Click **Save the configuration**.
10. In the **Job Schedule** section, click **Now**.
11. Click **Upgrade**.

On the Software Inventory page, the system displays the status of the upgrade in **Status**. Click the status of the Communication Manager device to view the logs and the description of the upgrade operation.

### Related links

[Upgrading Communication Manager 6.0, 6.1, or 6.2 to 6.3.100](#) on page 1453

[System Platform Templates Upgrade Configuration field descriptions](#) on page 1458

[Software Inventory field descriptions](#) on page 1460

## System Platform Templates Upgrade Configuration field descriptions

| Name                                     | Description                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Upgrade Source</b>                    | The source where you have the installation file. The source can be the remote server software library.                                                                                                                                                                                                                                                                     |
| <b>Available System Platform</b>         | The available System Platform for the upgrade.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                                                                                                                                  |
| <b>EPW file</b>                          | The EPW file available for the upgrade.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                                                                                                                                         |
| <b>Template Name</b>                     | The Communication Manager template available for the upgrade: <ul style="list-style-type: none"> <li>• CM_Simplex</li> <li>• CM_SurvRemoteEmbed</li> <li>• CM_SurvRemote</li> <li>• CM_onlyEmbed</li> <li>• CM_Duplex</li> </ul> The field applies only for Communication Manager Release 5.2.1 upgrade.<br>For Communication Manager Release 6.x, the field is read-only. |
| <b>CM/CMM Backup/Restore File Server</b> | The file server used for storing backup data during the upgrade.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                                                                                                                |
| <b>Authentication File</b>               | The link to authenticate the file.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                                                                                                                                              |
| <b>WebLM Server IP Address</b>           | The WebLM server IP address.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                                                                                                                                                    |
| <b>Communication Manager IP Address</b>  | The Communication Manager IP address. The Communication Manager IP address must be the same as the selected Communication Manager to be upgraded.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                               |
| <b>Upgrade To</b>                        | The Communication Manager template version that you want to upgrade to.                                                                                                                                                                                                                                                                                                    |
| <b>Branch Session Manager</b>            | The Branch Session Manager available for the upgrade. The <b>Branch Session Manager</b> IP address must be of the same name as mentioned in the <b>EPW</b> file.                                                                                                                                                                                                           |

*Table continues...*

| Name                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Branch Session Manager Login</b>               | The Branch Session Manager login name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Branch Session Manager Password</b>            | The Branch Session Manager password. The password must not exceed nine letters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Branch Session Manager Enrollment Password</b> | The Branch Session Manager enrollment password. The password must not exceed nine letters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Utility Server</b>                             | The Utility Services virtual application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Communication Manager</b>                      | The version of Communication Manager that you want to upgrade to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>System Platform Upgrade Version</b>            | The System Platform release upgrade that you want to upgrade to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>System Platform Update Version</b>             | The System Platform patch upgrade version that you want to update the version to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Utility Server IP Address</b>                  | <p>The Utility Services IP address. The name of <b>Utility Server IP Address</b> must be the same as mentioned in the <b>EPW</b> file.</p> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Auto Commit Upgrade</b>                        | <p>The option to automatically commit the template upgrade.</p> <ul style="list-style-type: none"> <li>If you select <b>Auto Commit Upgrade</b>, the system automatically upgrades System Platform.</li> </ul> <p> <b>Important:</b></p> <p>If you select <b>Auto Commit Upgrade</b>, you cannot roll back the template upgrade.</p> <ul style="list-style-type: none"> <li>If you do not select <b>Automatic Commit Upgrade</b>, the system displays <b>Waiting</b> or <b>RollBack</b> for <b>Commit</b> on the Software Inventory page.</li> </ul> <p>On the System Inventory page, click <b>More Actions</b> &gt; <b>Commit Template Upgrade</b>.</p> |
| <b>CM VM Kernel,Platform Patching</b>             | <p>The kernel patch or platform patch for the Communication Manager virtual machine.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>If selected, the kernel and platform patching must be performed implicitly on the Communication Manager virtual machine.</li> <li>If not selected, the kernel and platform patching must be performed manually on the Communication Manager virtual machine.</li> </ul> <p>For more information, see <i>Deploying Avaya Aura® Communication Manager on System Platform</i>.</p>                                                                                                                    |
| <b>CM VM Platform Patch</b>                       | The platform patch for the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>CM VM Kernel Patch</b>                         | The kernel patch for the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table continues...

| Name                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Override Recommended Failure</b> | <p>The checkbox that specifies whether the system must override any recommended preupgrade check failure that occurs during the element upgrade. When you select this checkbox, the system tries to upgrade the element.</p> <p> <b>Note:</b></p> <p>You must select <b>Override Recommended Failure</b> if one or more of the earlier recommended preupgrade checks have failed.</p> |

 **Note:**

If a version is unavailable in the library, the system displays a warning for the following fields:

- **Upgrade To**
- **Communication Manager**
- **System Platform Upgrade Version**
- **System Platform Update Version**

| Button          | Description                             |
|-----------------|-----------------------------------------|
| <b>Done</b>     | To save the information that you enter. |
| <b>Reset</b>    | To clear the values that you enter.     |
| <b>Now</b>      | To begin the upgrade.                   |
| <b>Schedule</b> | To schedule the upgrade for later.      |
| <b>Cancel</b>   | To cancel the upgrade.                  |

## Software Inventory field descriptions

| Name                            | Description                           |
|---------------------------------|---------------------------------------|
| <b>Adjust column width</b>      |                                       |
| <b>Select</b>                   | The option to select a group.         |
| <b>Name</b>                     | The name of the device.               |
| <b>Release</b>                  | The release state.                    |
| <b>Update</b>                   | The update state.                     |
| <b>Pre-Upgrade Check Status</b> | The status of the preupgrade check.   |
| <b>IP Address</b>               | The IP address.                       |
| <b>Type</b>                     | The device type.                      |
| <b>Sw Release</b>               | The software release.                 |
| <b>Status</b>                   | The status of the device for upgrade. |
| <b>Location</b>                 | The location of the device.           |
| <b>Family</b>                   | The family of the device.             |

| Button                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Get inventory &gt; Now</b>                 | To get the components of the device software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Get inventory &gt; Schedule</b>            | To get the components of the device software at a later time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Analyze &gt; Analyze All Now</b>           | To analyze whether any new firmware for all device software is available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Analyze &gt; Analyze All Scheduled</b>     | To analyze at a later time whether any new firmware for all device software is available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Analyze &gt; Analyze Selected Now</b>      | To analyze whether any new firmware for the selected device is available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Analyze &gt; Analyze Selected Schedule</b> | To analyze at a later time whether any new firmware for the selected device is available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Download</b>                               | To download the required files for one or more devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Pre-upgrade Check</b>                      | To display the system requirement for an upgrade as follows: <ul style="list-style-type: none"> <li>• The required bandwidth of the selected device.</li> <li>• The required entitlements downloaded by the System Manager and the selected device.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Upgrade</b>                                | To upgrade the device template.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>More Actions &gt; Commit</b>               | Prompts you to save the changes you made to the selected Communication Manager, Gateway, or the loads the previous release on the selected Communication Manager, System Platform template, Gateway template. Do one on the following actions; <ul style="list-style-type: none"> <li>• <b>Now:</b> To commit the upgrades to the latest release on the selected Communication Manager, Gateway, or the System Platform template.</li> <li>• <b>Later:</b> To commit the upgrades to the latest release on the selected Communication Manager, Gateway, or the System Platform template at a later time.</li> <li>• <b>Cancel:</b> To cancel the upgrades to the latest release on the selected Communication Manager, Gateway, or the System Platform template.</li> </ul> |
| <b>More Actions &gt; Rollback</b>             | Loads the previous release on the selected Communication Manager, System Platform template, gateway. The options are: <ul style="list-style-type: none"> <li>• <b>Now:</b> To rollback the upgrades to the previous release on the selected Communication Manager, Gateway, or the System Platform template.</li> <li>• <b>Later:</b> To rollback the upgrades to the previous release on the selected Communication Manager, gateway, or the System Platform template at a later time.</li> <li>• <b>Cancel:</b> To cancel the rollback of the upgrades to the previous release on the selected Communication Manager, gateway, or the System Platform template.</li> </ul>                                                                                                |

*Table continues...*

| Button                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>More Actions &gt; Reset</b>                   | <p>Restarts the selected Communication Manager, or Gateway. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Now:</b> To restart the selected Communication Manager or Gateway.</li> <li>• <b>Later:</b> To restart the selected Communication Manager or Gateway.</li> <li>• <b>Cancel:</b> To cancel the restart on the selected Communication Manager or Gateway.</li> </ul> <p>Reset operation is service affecting, with higher levels being increasingly destructive that can close the SAT login. Certain conditions can result in a higher reset level than the reset requested.</p> |
| <b>More Actions &gt; Cancel Template Upgrade</b> | <p>Cancels the System Manager template upgrade. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Now:</b> To cancel the template upgrade on the selected System Platform solution template.</li> <li>• <b>Later:</b> To cancel the template upgrade on the selected System Platform solution template at a later time.</li> <li>• <b>Cancel:</b> To cancel the cancel template upgrade on the selected System Platform solution template.</li> </ul>                                                                                                                                         |
| <b>More Actions &gt; Backup CM/CMM</b>           | <p>Displays the Backup Configuration page where you can create a backup of Communication Manager 5.2.1 that you want to upgrade.</p> <p>For more information see, Backing up Communication Manager.</p> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p>                                                                                                                                                                                                                                                                                                                       |
| <b>Advanced Search</b>                           | Displays fields where you can specify the criteria for searching a group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Filter: Enable</b>                            | Displays fields where you can set the filter criteria. This button is a toggle button.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Filter: Disable</b>                           | Hides the column filter fields without resetting the filter criteria. This button is a toggle button.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Filter: Clear</b>                             | Clears the filter criteria.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Filter: Apply</b>                             | Filters groups based on the criteria.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Select: None</b>                              | Clears all check boxes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Icon                                                                                | Description                      |
|-------------------------------------------------------------------------------------|----------------------------------|
|  | Refreshes the group information. |

## Criteria section

Click **Advanced Search** to view this section. You can find the **Advanced Search** link in the upper-right corner of the page.

| Name | Description |
|------|-------------|
|------|-------------|

*Table continues...*



|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criteria</b> | <p>The criteria for search operation. The page displays the following fields:</p> <ul style="list-style-type: none"> <li>• <b>Field 1:</b> The list of criteria to search groups.</li> <li>• <b>Field 2:</b> The list of operators for evaluating the expression. This list of operators depends on the criterion that you selected in <b>Field 1</b>.</li> <li>• <b>Field 3:</b> The value of the search criterion. The Software Inventory service retrieves and displays the devices that match this value.</li> </ul> |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Icon | Description                                                                                          |
|------|------------------------------------------------------------------------------------------------------|
| +    | Adds a row after <b>Field 1</b> , <b>Field 2</b> , and <b>Field 3</b> to add more search conditions. |
| -    | Deletes the row with the search conditions.                                                          |

| Button        | Description                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Clear</b>  | Clears the search value that you entered in <b>Field 3</b> .                                                        |
| <b>Search</b> | Searches the group based on the specified search conditions, and displays the results in the <b>Groups</b> section. |
| <b>Close</b>  | Cancels the search operation, and hides the <b>Criteria</b> section.                                                |

## Upgrading Communication Manager 5.2.1

### Communication Manager Release 5.2.1 upgrade

You can upgrade Communication Manager Release 5.2.1 to Release 6.3.100 on a different server. For example:

- You can upgrade Communication Manager Release 5.2.1 running on a different server. On the CM Upgrade Configuration page, you must click **Upgrade** for the system to perform the upgrade. For more information, see “Upgrading to Communication Manager on a different server”.
- You must perform **Get Inventory** to get the latest state of System Platform before you upgrade Communication Manager Release 5.2.1 to Release 6.3.100 on a different server. You must perform the step in the following scenario:
  1. On your system, you have added System Platform to the inventory
  2. After adding System Platform, you have applied latest software patch from the System Platform web console.

#### Related links

[Upgrading Communication Manager 5.2.1 to Release 6.3.100 on a different server](#) on page 1472

## Communication Manager 5.2.1 upgrade checklist

| No. | Task                                                                                                                                                                                                       | References                                                                                                                                                                                                                                                                          | ✓ |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1.  | Install System Platform and the required patch on the supported server.                                                                                                                                    | —                                                                                                                                                                                                                                                                                   |   |
| 2.  | Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page.                                                                                       | <a href="#">Discovering elements</a> on page 899                                                                                                                                                                                                                                    |   |
| 3.  | Configure user settings.                                                                                                                                                                                   | <a href="#">Configuring user settings</a> on page 1287                                                                                                                                                                                                                              |   |
| 4.  | Create a remote software library.                                                                                                                                                                          | <a href="#">Creating a software library</a> on page 1303                                                                                                                                                                                                                            |   |
| 5.  | Record the server data for Communication Manager 5.2.1 in the worksheet.                                                                                                                                   | For more information about the following, see <i>Upgrading Avaya Aura® Communication Manager</i> : <ul style="list-style-type: none"> <li>Recording the configuration screens.</li> <li>Worksheet for upgrading Communication Manager to simplex and embedded templates.</li> </ul> |   |
| 6.  | Create the authorization file for System Platform, and store the file in <b>My Computer</b> .                                                                                                              | For more information, contact the Avaya support team.                                                                                                                                                                                                                               |   |
| 7.  | Create the new EPW file for the Communication Manager selected for upgrade, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server. | For more information, contact the Avaya support team.                                                                                                                                                                                                                               |   |
| 8.  | Get the WebLM server IP address for licensing.                                                                                                                                                             | For more information, contact the Avaya support team.                                                                                                                                                                                                                               |   |
| 9.  | Get the inventory for Communication Manager 5.2.1.                                                                                                                                                         | <a href="#">Get inventory software inventory</a> on page 1443                                                                                                                                                                                                                       |   |
| 10. | Analyze the software.                                                                                                                                                                                      | <a href="#">Analyzing the software for software inventory</a> on page 1445                                                                                                                                                                                                          |   |
| 11. | Download the related firmware for the Communication Manager upgrade.                                                                                                                                       | <a href="#">Downloading the software for software inventory</a> on page 1445                                                                                                                                                                                                        |   |
| 12. | Perform a preupgrade check.                                                                                                                                                                                | <a href="#">Performing the preupgrade check</a> on page 1446                                                                                                                                                                                                                        |   |
| 13. | Perform the upgrade.                                                                                                                                                                                       | <a href="#">Upgrading Communication Manager 5.2.1</a> on page 1472                                                                                                                                                                                                                  |   |
| 14. | Verify that the upgrade is successful.                                                                                                                                                                     | <a href="#">Verifying the upgrade</a> on page 1455                                                                                                                                                                                                                                  |   |

Table continues...

| No. | Task                                                                                               | References                                         | ✓ |
|-----|----------------------------------------------------------------------------------------------------|----------------------------------------------------|---|
| 15. | Validate that the Communication Manager 5.2.1 server data that is restored on 6.3.100 is complete. | <a href="#">Verifying the upgrade</a> on page 1455 |   |

**Related links**

[Device list](#) on page 901

## Backing up Communication Manager or Communication Manager Messaging

**Before you begin**

- Get the inventory.
- Analyze the software.
- Download the software.

**About this task**

Perform the routine backup of Communication Manager 5.2.1 and Communication Manager Messaging. You also need to take a backup before you upgrade Communication Manager in the semi-automated mode.

**Procedure**

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the template that you want to upgrade and click **More Actions > Backup CM/CMM**.
6. On the Backup Configuration page, do the following:
  - a. From the list of available elements, select the element that you want to upgrade.
  - b. In the Upgrade Operations section, in **CM/CMM Backup/Restore File Server**, click the appropriate file server where you want to take the backup.
  - c. Select the **Ready for Upgrade** check box.
 

The system marks the Communication Manager device used for upgrade. Communication Manager becomes unavailable for any administrative operations such as incremental synchronization.
7. In the **Job Schedule > Schedule Job** section, do one of the following:
  - To perform the backup immediately, click **Now**.
  - To perform the backup later, click **Later**.

8. Click **Backup CM/CMM**.**Result**

On successful completion of the backup, if you have selected the **Ready for Upgrade** check box, Communication Manager:

- Shuts down, except when running on the S8300D server
- Becomes nonoperational until the upgrade is complete

**Next steps**

You can start the upgrade after successful completion of the backup.

To start the upgrade, on the CM Upgrade Configuration page, click **Upgrade**.

**Backup Configuration field descriptions****Upgrade Operations**

| Name                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CM/CMM Backup/Restore File Server</b> | The backup file server address for backup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Ready for Upgrade</b>                 | <p>The option to select the Communication Manager device for upgrade. Communication Manager becomes unavailable for any administrative operations such as incremental synchronization. On successful completion of the backup, Communication Manager shuts down, except when running on the S8300D server, and becomes nonoperational until the upgrade is complete.</p> <p> <b>Note:</b></p> <p>When you select the check box, system does not refresh this Communication Manager when you perform the get inventory operation. You must clear the check box to refresh Communication Manager during the get inventory operation.</p> |

| Button                        | Description                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Save the configuration</b> | Saves the backup configuration with the latest modifications.                                           |
| <b>Clear configuration</b>    | Resets the backup configuration page to the default settings.                                           |
| <b>Backup CM/CMM</b>          | Creates a backup copy of the selected Communication Manager or Communication Manager Messaging element. |
| <b>Cancel</b>                 | Cancels the backup operation and returns to the CM Backup Configuration page.                           |

**CM Upgrade Configuration field descriptions**

The following table is updated when you choose the upgrade, update, or license authentication operations for Communication Manager. You can upgrade or update multiple Communication Manager devices simultaneously.

| Name                            | Description                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Element Name</b>             | The name of Communication Manager.                                                                                                                   |
| <b>IP Address</b>               | The IP address of the Communication Manager device.                                                                                                  |
| <b>Software Version</b>         | The software version of Communication Manager that you selected.                                                                                     |
| <b>Server Status</b>            | Specifies whether Communication Manager is active or standby. The <b>Server Status</b> field is applicable only to the duplex Communication Manager. |
| <b>Operation</b>                | The upgrade operation that you want to perform for the Communication Manager devices that you choose.                                                |
| <b>Release</b>                  | The current version of Communication Manager.                                                                                                        |
| <b>SAMP/MPC</b>                 | The SAMP firmware that is available.                                                                                                                 |
| <b>CM Service Pack</b>          | The Communication Manager service pack available.                                                                                                    |
| <b>SES Service Pack</b>         | The SES service pack available.                                                                                                                      |
| <b>Kernel Update</b>            | The kernel update available.                                                                                                                         |
| <b>Platform/Security Update</b> | The platform or security update available.                                                                                                           |
| <b>License File</b>             | The license file that you downloaded for the upgrade operation.                                                                                      |
| <b>Authentication File</b>      | The authentication file that you downloaded for the upgrade operation.                                                                               |

## Upgrade operations

The system displays the following fields for upgrading Communication Manager 5.x to Communication Manager 5.2.1.

| Name             | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operation</b> | The operation that you want to perform. The options are: <ul style="list-style-type: none"> <li>• <b>Copy Release:</b> To copy the release file from a CD-ROM or a URL.</li> <li>• <b>Install Release:</b> To install the Communication Manager release that you selected.</li> <li>• <b>Copy &amp; Install Release:</b> To copy the installation file and install the Communication Manager release using the file.</li> </ul> |
| <b>Source</b>    | The source the installation file is made available. The source can be a remote server or CD-ROM on Communication Manager.                                                                                                                                                                                                                                                                                                       |
| <b>Method</b>    | The remote server protocol. The <b>Method</b> field applies only for a remote server.<br><br>For SCP, FTP, and SFTP, provide the user name, password, host name, and directory name.<br><br>For HTTP and HTTPS, provide the URL and proxy details.                                                                                                                                                                              |

*Table continues...*

| Name                       | Description                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto Commit Upgrade</b> | <p>The option to specify if a backup of the current release is available. The options are:</p> <ul style="list-style-type: none"> <li>• <b>Yes:</b> A backup of the current release is available. Rollback is not possible if you select yes.</li> <li>• <b>No:</b> A backup of the current release is unavailable. Rollback is possible if you select no.</li> </ul> |

The system displays the following fields for upgrading the Communication Manager 5.2.1. to Communication Manager 6.x and later.

| Name                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Upgrade Source</b>            | <p>The source where the installation file is available. The can be Software Library that can be used for semi-automated upgrade.</p> <p>You must install System Platform and the latest software patch and click <b>Upgrade</b> for the system to perform the upgrade.</p> <p> <b>Note:</b></p> <p>Based on the <b>Upgrade Source</b> you select, the system displays different sets of templates in the <b>Select Templates</b> field.</p>                                                                                                                                                                                                                           |
| <b>Available System Platform</b> | <p>System Platform that is available for the upgrade.</p> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>EPW file</b>                  | <p>The complete path of EPW file that is available for upgrade.</p> <p>For example, <code>http://&lt;file-server&gt;/epw.zip</code>.</p> <p>This valid file server must support HTTP or HTTPS protocol. You must copy the EPW file on the server and the EPW file must be made available on the server before you begin the upgrade.</p> <p>You require the EPW file for the solution template upgrade. The file consists of the IP address and network details of System Platform and virtual machines.</p> <p>Ensure that you gain access to the EPW file from System Manager and System Platform at the http url that is specified in the field.</p> <p>You can create the EPW file by using EPW installer tool available with System Platform.</p> |

*Table continues...*

| Name                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Select Template</b>                   | <p>The Communication Manager template available for the upgrade. The options are:</p> <ul style="list-style-type: none"> <li>• CM_Simplex</li> <li>• CM_SurvRemoteEmbed</li> <li>• CM_SurvRemote</li> <li>• CM_onlyEmbed</li> <li>• CM_Duplex</li> </ul> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p> <p> <b>Note:</b></p> <p>The system displays different sets of templates in the <b>Select Template</b> field based on the <b>Upgrade Source</b> that you select.</p> <p>For Communication Manager Release 6.x, the field is read-only.</p> <p> <b>Note:</b></p> <p>Based on the template that you select, the system displays appropriate fields.</p> |
| <b>CM/CMM Backup/Restore File Server</b> | <p>The file server that is used to store the backup data during the upgrade.</p> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p> <p>On the Backup Configuration page, if you select <b>Ready For Upgrade</b>, the system displays the file server address where the backup data is saved.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Authentication File</b>               | <p>The link to authenticate the file.</p> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>WebLM Server IP Address</b>           | <p>The IP address of the WebLM server.</p> <p>The field applies only for Communication Manager Release 5.2.1 upgrade.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Vlan Id</b>                           | <p>The IP address of the VLAN circuit pack.</p> <p> <b>Note:</b></p> <p>The system displays the field only when you select <b>Flash Drive</b> in the <b>Upgrade Source</b> field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Dom0 Hostname</b>                     | <p>The host name of the Domain-0 virtual machine.</p> <p> <b>Note:</b></p> <p>The system displays the field only when you select <b>Flash Drive</b> in the <b>Upgrade Source</b> field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

*Table continues...*

| Name                                              | Description                                                                                                                                                                                                                                                                         |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cdom Hostname</b>                              | The host name of the System Platform console domain virtual machine.<br> <b>Note:</b><br>The system displays the field only when you select <b>Flash Drive</b> in the <b>Upgrade Source</b> field. |
| <b>Services Hostname</b>                          | The host name of the Services virtual machine.<br> <b>Note:</b><br>The system displays the field only when you select <b>Flash Drive</b> in the <b>Upgrade Source</b> field.                       |
| <b>SP Root Password</b>                           | The password for the System Platform root user.<br> <b>Note:</b><br>The system displays the field only when you select <b>Flash Drive</b> in the <b>Upgrade Source</b> field.                      |
| <b>Ldap Root Password</b>                         | The password for the root user of the LDAP directory server.<br> <b>Note:</b><br>The system displays the field only when you select <b>Flash Drive</b> in the <b>Upgrade Source</b> field.         |
| <b>Communication Manager IP Address</b>           | The Communication Manager IP address. The Communication Manager IP address must be the same as the Communication Manager system that you selected for upgrade.<br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                           |
| <b>Upgrade To</b>                                 | The device to which you want to upgrade.                                                                                                                                                                                                                                            |
| <b>Branch Session Manager</b>                     | The Branch Session Manager available for the upgrade. The Branch Session Manager IP address must be the same that is mentioned in the <b>EPW</b> file.                                                                                                                              |
| <b>Branch Session Manager Login</b>               | The Branch Session Manager login.                                                                                                                                                                                                                                                   |
| <b>Branch Session Manager Password</b>            | The Branch Session Manager password. The password must not exceed nine letters.                                                                                                                                                                                                     |
| <b>Branch Session Manager Enrollment Password</b> | The Branch Session Manager enrollment password. The password must not exceed nine letters.                                                                                                                                                                                          |
| <b>Utility Server</b>                             | The Utility Services available for the upgrade.                                                                                                                                                                                                                                     |
| <b>Communication Manager</b>                      | The available Communication Manager.                                                                                                                                                                                                                                                |
| <b>System Platform Upgrade Version</b>            | The available System Platform upgrade version for the upgrade.                                                                                                                                                                                                                      |
| <b>System Platform Update Version</b>             | The available System Platform update version for the upgrade.                                                                                                                                                                                                                       |

*Table continues...*



| Name                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Utility Server IP Address</b>      | The Utility Services IP address. The IP address must be the same as the IP address mentioned in the EPW file.<br><br>The field applies only for Communication Manager Release 5.2.1 upgrade.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Auto Commit Upgrade</b>            | The field to specify if a backup of the current release is available. The options are: <ul style="list-style-type: none"> <li>• <b>Yes:</b> If you do not require a backup of the current release. Rollback is not possible if you select Yes.</li> <li>• <b>No:</b> If you require a backup of the current release. You can perform a rollback operation if you select No.</li> </ul>                                                                                                                                                                                                                       |
| <b>CM VM Kernel,Platform Patching</b> | The kernel patch or platform patch for the Communication Manager virtual machine.<br><br> <b>Note:</b> <ul style="list-style-type: none"> <li>• If selected, the kernel and platform patching must be performed implicitly on the Communication Manager virtual machine.</li> <li>• If not selected, the kernel and platform patching must be performed manually on the Communication Manager virtual machine.</li> </ul> For more information, see <i>Deploying Avaya Aura® Communication Manager on System Platform</i> . |
| <b>CM VM Platform Patch</b>           | The platform patch for the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>CM VM Kernel Patch</b>             | The kernel patch for the Communication Manager virtual machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Override Recommended Failure</b>   | The option that specifies whether the system must override any recommended preupgrade check failure that occurs during the element upgrade. When you select this option, the system continues with upgrade even when a recommended preupgrade check fails.<br><br> <b>Note:</b> <p>Select <b>Override Recommended Failure</b> if one or more of the earlier recommended preupgrade checks have failed.</p>                                                                                                                |

## Update Operations

| Name                            | Description                                                               |
|---------------------------------|---------------------------------------------------------------------------|
| <b>CM Service Pack</b>          | The Communication Manager service pack version to which you are entitled. |
| <b>SES Service Pack</b>         | The SES service pack update to which you are entitled.                    |
| <b>Kernel Update</b>            | The kernel update to which you are entitled.                              |
| <b>Platform/Security Update</b> | The platform or security update to which you are entitled.                |

## License Authentication Operations

| Name                              | Description                                                   |
|-----------------------------------|---------------------------------------------------------------|
| <b>Import License File</b>        | The license file that you must select for the upgrade.        |
| <b>Import Authentication File</b> | The authentication file that you must select for the upgrade. |

| Button                        | Description                                                                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>Save Configuration</b>     | To save the configuration. You can save the configuration details for multiple Communication Manager devices before upgrading. |
| <b>Clear Configuration</b>    | To clear the configuration that you have chosen.                                                                               |
| <b>Proceed to Job Summary</b> | To view the summary of the configuration that you have chosen.                                                                 |
| <b>Commit</b>                 | To perform the upgrade operation.                                                                                              |
| <b>Cancel</b>                 | To cancel your current operation, and go to the previous page.                                                                 |

## Upgrading Communication Manager 5.2.1 to Release 6.3.100 on a different server

### Before you begin

- Install the latest System Platform release and the latest service pack on the supported server.  
For more information, see Hardware requirement checks during preupgrade check.

- The recommended System Platform must be on the same subnetwork as Communication Manager 5.2.1.

- Record the server data for Communication Manager 5.2.1 in the worksheet for upgrading Communication Manager to simplex and embedded templates.

For more information, see Recording the configuration screens, and Worksheet for upgrading Communication Manager to simplex and embedded templates, see *Upgrading Avaya Aura® Communication Manager*.

The system backs up most of the server data and restores the data after the upgrade. You must verify and complete the configuration after the upgrade is complete.

- Create the authorization file for System Platform, and store the file in **My Computer**.

For more information, contact the Avaya support team.

- Create the EPW file for the Communication Manager selected for upgrade, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server.

For more information, contact the Avaya support team.

- Get the WebLM server IP address that is mandatory for licensing.

For more information, contact the Avaya support team.

- Get the inventory for Communication Manager 5.2.1.

The get inventory operation ensures that the system reflects the exact state of the device in Software Inventory.

- Analyze the software.
- Download the related firmware for the Communication Manager upgrade.
- Run the preupgrade check.

### About this task

Use the procedure to upgrade Communication Manager 5.2.1 to Release 6.3.100 on a different server.

#### Important:

For a duplex, first upgrade the standby Communication Manager and then the active Communication Manager.

When you select a Communication Manager on which Communication Manager Messaging is enabled, the Communication Manager Messaging device updates to the latest version after the upgrade.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 5.2.1 device that you want to upgrade.
6. **(Optional)** For a semiautomated upgrade, perform the following:
  - a. Create a backup.
  - b. To upgrade on a different server, clear the **Ready for Upgrade** check box.

For more information, see [Backing up Communication Manager or Communication Manager Messaging](#) on page 1465

7. Click **Upgrade**.
8. On the CM Upgrade Configuration page, perform the following:
  - a. Select the Communication Manager 5.2.1 device to which you want to upgrade.
  - b. Provide the HTTP or HTTPS path for the EPW file.
  - c. Browse and select the authentication file.
  - d. In the Upgrade Operations section, complete the fields.
    - a. For semi automated upgrade, in the **Upgrade Source** field, select **Software Library**.
    - b. In the **Available System Platform** field, select the System Platform device that you manually installed and added to System Manager.

For more information, see [Add Communication Manager field descriptions](#) on page 947.

c. In the **Select Template** field, select a template.

For more information, see [CM Upgrade Configuration field descriptions](#) on page 1466.

e. Click **Save the configuration**.

9. In the Job Schedule section, perform one of the following:

- To upgrade the device, click **Now**.
- To upgrade the device at a later time, click **Later**.

10. Click **Upgrade**.

The Software Inventory page displays the status of the upgrade in **Status**.

11. To view the logs and the description of the upgrade operation, click the status of the Communication Manager device.

### Next steps

- Verify that the upgrade is successful.
- Validate that the Communication Manager 5.2.1 server data that is restored on the new system is complete.

For more information, see [Verifying the upgrade](#) on page 1455.

### Related links

[Analyze software](#) on page 1444

[CM Upgrade Configuration field descriptions](#) on page 1466

[Analyzing the software](#) on page 1445

[Getting inventory](#) on page 1443

[Creating a software library](#) on page 1303

[Performing a preupgrade check](#) on page 1446

[Preupgrade checks](#) on page 1448

[Sample scenario to upgrade Communication Manager Release 5.2.1 to 6.3.100 on a different server](#) on page 1474

[Hardware requirement checks during a preupgrade check](#) on page 1450

[Communication Manager 5.2.1 upgrade checklist](#) on page 1464

[Device list](#) on page 901

## Sample scenario to upgrade Communication Manager Release 5.2.1 to 6.3.100 on a different server

To upgrade Communication Manager Release 5.2.1 to 6.3.100 on a different server, do the following:

1. Perform the [Preupgrade tasks](#) on page 1475.
2. Perform the [Upgrading Communication Manager 5.2.1 to 6.3.100](#) on page 1476.
3. Perform [Verifying the upgrade](#) on page 1455.

## Preupgrade tasks

| No. | Task                                                                                                                                                                                                              | References                                                                                                                                                                                                                                                                          | ✓ |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 1.  | Discover the devices that you want to upgrade by enabling SNMP or adding from Discovery on the Manage Elements page.                                                                                              | <a href="#">Discovering elements</a> on page 899                                                                                                                                                                                                                                    |   |
| 2.  | Configure user settings.                                                                                                                                                                                          | <a href="#">Configuring user settings</a> on page 1287                                                                                                                                                                                                                              |   |
| 3.  | Create a remote software library.                                                                                                                                                                                 | <a href="#">Creating a software library</a> on page 1303                                                                                                                                                                                                                            |   |
| 4.  | Install the latest System Platform software on the supported server.<br><br>Visit the Avaya support site for the latest available software.                                                                       | <a href="#">Hardware requirement checks during preupgrade check</a> on page 1450                                                                                                                                                                                                    |   |
| 5.  | Record the server data for Communication Manager 5.2.1 in the worksheet for upgrading Communication Manager to simplex and embedded templates.                                                                    | For more information about the following, see <i>Upgrading Avaya Aura® Communication Manager</i> : <ul style="list-style-type: none"> <li>Recording the configuration screens.</li> <li>Worksheet for upgrading Communication Manager to simplex and embedded templates.</li> </ul> |   |
| 6.  | Create the authorization file for System Platform, and store the file in <b>My Computer</b> .                                                                                                                     | For more information, contact the Avaya support team.                                                                                                                                                                                                                               |   |
| 7.  | Create a new EPW file for the Communication Manager instance selected for upgrade, and provide all credentials to the EPW file including System Platform details. Store the EPW file on the HTTP or HTTPS server. | For more information, contact the Avaya support team.                                                                                                                                                                                                                               |   |
| 8.  | Get the WebLM server IP address for licensing.                                                                                                                                                                    | For more information, contact the Avaya support team.                                                                                                                                                                                                                               |   |
| 9.  | Get the inventory for Communication Manager 5.2.1.                                                                                                                                                                | <a href="#">Get inventory software inventory</a> on page 1443                                                                                                                                                                                                                       |   |
| 10. | Analyze the software.                                                                                                                                                                                             | <a href="#">Analyzing the software for software inventory</a> on page 1445                                                                                                                                                                                                          |   |
| 11. | Download the related firmware for the Communication Manager upgrade.                                                                                                                                              | <a href="#">Downloading the software for software inventory</a> on page 1445                                                                                                                                                                                                        |   |
| 12. | Perform the preupgrade check.                                                                                                                                                                                     | <a href="#">Performing the preupgrade check</a> on page 1446                                                                                                                                                                                                                        |   |

## Upgrading Communication Manager 5.2.1 to 6.3.100

### Before you begin

Complete the preupgrade tasks.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 5.2.1 device that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, perform the following:
  - a. Provide the HTTP or HTTPS path for the EPW file.
  - b. Browse and select the authentication file on **My Computer** in the field required.
  - c. In the Upgrade Operations section, complete the fields.  
For more information, see CM Upgrade Configuration field description.
  - d. Click **Save the configuration**.
  - e. In the **Job Schedule** section, click **Now**.
8. Click **Upgrade**.  
The Software Inventory page displays the status of the upgrade in **Status**.
9. To view the logs and the upgrade details, click the status of the Communication Manager device.

## Server support for Communication Manager Release 5.2.1 to 6.3.100 upgrades

| Existing CM 5.2.1 server | Possible CM 6.3.100 templates during software and hardware upgrades | Servers compatible for upgrade to CM 6.3.100 |
|--------------------------|---------------------------------------------------------------------|----------------------------------------------|
| HP DL360 G7              | CM_Simplex<br>CM_Duplex<br>CM_SurvRemote                            | Yes                                          |

*Table continues...*

| Existing CM 5.2.1 server | Possible CM 6.3.100 templates during software and hardware upgrades | Servers compatible for upgrade to CM 6.3.100 |
|--------------------------|---------------------------------------------------------------------|----------------------------------------------|
| HP DL360 G8              | CM_Simplex<br>CM_Duplex<br>CM_SurvRemote                            | Yes                                          |
| S8300D                   | CM_onlyEmbed<br>CM_SurvRemoteEmbed                                  | Yes                                          |
| S8510                    | CM_Simplex<br>CM_SurvRemote                                         | Yes                                          |
| S8800                    | CM_Simplex<br>CM_Duplex<br>CM_SurvRemote                            | Yes                                          |
| S8300C                   | CM_Simplex<br>CM_Duplex<br>CM_SurvRemote                            | No                                           |
| S8300B                   | CM_Simplex<br>CM_Duplex<br>CM_SurvRemote                            | No                                           |
| S8400                    | CM_Simplex                                                          | No                                           |
| S8400B                   | CM_Simplex                                                          | No                                           |
| S8500                    | CM_Simplex<br>CM_SurvRemote                                         | No                                           |
| S8500A                   | CM_Simplex<br>CM_SurvRemote                                         | No                                           |
| S8500B                   | CM_Simplex<br>CM_SurvRemote                                         | No                                           |
| S8500C                   | CM_Simplex<br>CM_SurvRemote                                         | No                                           |
| S8710                    | CM_Duplex<br>CM_SurvRemote                                          | No                                           |
| S8720                    | CM_Duplex<br>CM_SurvRemote                                          | No                                           |
| S8730                    | CM_Duplex<br>CM_SurvRemote                                          | No                                           |

---

## Upgrading TN boards

### Before you begin

For TN boards, perform the following:

- Get the inventory.
- Analyze the firmware.
- Download the firmware.

You cannot upgrade the TN board if the TN board:

- Is in the nonupgradable  **State**
- Has a Virtual IP address

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the Communication Manager devices that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, click the TN Boards tab.
8. Select the TN board that you want to upgrade.
9. Download the upgrade file to the software library.

The state of the TN board changes to .

10. Click **Upgrade**.

The system displays the status of the upgrade operation as RUNNING.

11. Click the status to view the description of the upgrade operation.

### Related links

[Analyze software](#) on page 1444

---

## Upgrading media gateways and media modules

### About this task

According to the compatibility matrix, you can upgrade Media Gateway/Media Module from:

- Higher Release to Lower Release



- Lower Release to Higher Release

Therefore, in Solution Deployment Manager, if Gateways/Media Modules are on latest firmware release on the Upgrade Management page and if any older firmware artifact(s) already downloaded in Software Library then the **Update Status** column displays **Ready for Upgrade** on the Upgrade Management page. You can see the compatibility matrix on Avaya Support website.

If a Avaya MP160 Media Module is added in System Manager on the **Inventory > Manage Elements** > page and its device type is displaying as **Other** then:

1. Upgrade to System Manager 7.1.3.5 (if the system is on the System Manager 7.1.x load) or Release 8.1.1 (if the system is on System Manager 8.1.x load)
2. Click **Refresh Elements** operation against the Media Module

By doing this, the system starts displaying the device type as **Avaya MP160** instead of **Other** on the Upgrade Management and Manage Elements pages.

 **Note:**

System Manager Release 8.0.x does not have this change. Therefore, on the System Manager 8.0.x system the device type of Avaya MP160 Media Modules is displayed as **Other**.

### Before you begin

- Obtain the inventory for the media gateways.
- Analyze the software.
- Download the software.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the Communication Manager devices that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, click the Gateway tab.
8. Download the upgrade file to the software library.

The **Upgrade** is enabled only if the **State** of the media gateway state changes to ready to update .

The device state changes to ready to update .

9. Select the media gateway that you want to upgrade.
10. Click **Upgrade**.
11. On the Gateway Upgrade Configuration page, click **Now**.

The system displays the status of the upgrade job as **RUNNING**.

12. Click the status to view the description of the upgrade job.

### Related links

[Protocol matrix for upgrades](#) on page 1486

## G430 Branch Gateway and G450 Branch Gateway multistep upgrade overview

Direct upgrade of G430 Branch Gateway and G450 Branch Gateway is not supported for certain versions. You must upgrade the gateway through specific intermediate versions. The following table displays the supported upgrade path of G430 Branch Gateway and G450 Branch Gateway:

| Upgrade/<br>Downgrade | To version          |                     |                      |                      |                                     |                                     |
|-----------------------|---------------------|---------------------|----------------------|----------------------|-------------------------------------|-------------------------------------|
| From<br>version       | <= 36.xx            | 37.xx               | 38.18 to<br>38.20.x  | 38.21.0              | 39.5.0 and<br>later                 | 40.xx                               |
| <= 36.xx              | Direct<br>Upgrade   | Direct<br>Upgrade   | Upgrade via<br>37.xx | Upgrade via<br>37.xx | Upgrade via<br>37.xx and<br>38.21.0 | Upgrade via<br>37.xx and<br>38.21.0 |
| <= 37. xx             | Direct<br>Downgrade | Direct<br>Upgrade   | Direct<br>Upgrade    | Direct<br>Upgrade    | Upgrade via<br>38.21.0              | Upgrade via<br>38.21.0              |
| 38.18 –<br>38.20.x    | Direct<br>Downgrade | Direct<br>Downgrade | Direct<br>Upgrade    | Direct<br>Upgrade    | Upgrade via<br>38.21.0              | Upgrade via<br>38.21.0              |
| 39.5.0                | Direct<br>Downgrade | Direct<br>Downgrade | Direct<br>Downgrade  | Direct<br>Downgrade  | Direct<br>Upgrade                   | Direct<br>Upgrade                   |
| 40.xx                 | Direct<br>Downgrade | Direct<br>Downgrade | Direct<br>Downgrade  | Direct<br>Downgrade  | Direct<br>Downgrade                 | Direct<br>Upgrade                   |

For example, if G430 Branch Gateway is currently on version 36.8.0 and must be upgraded to 39.5.0, then first upgrade the gateway to 37.xx of version such as 37.38.0 or 37.41.0. Then upgrade to 38.21.0, and then to 39.5.0. Therefore, the upgrade path is 36.8.0 > 37.xx > 38.21.0 > 39.5.0.

Solution Deployment Manager supports this multistep upgrade and updates it automatically based on the current version of the gateway and the selected Upgrade to version. But Solution Deployment Manager requires that you download the intermediate versions for the upgrade path in the same software library where the selected Upgrade to version is present. Solution Deployment Manager then automatically upgrades the gateway through the intermediate versions and up to the selected Upgrade to version.

If you perform a gateway upgrade through Solution Deployment Manager, the system displays an error message. This message is irrespective of the availability of the required intermediate version in the selected software library (**Upgrade Source**) on the Upgrade Configuration page.

**Element Configuration** \*

**General Configuration Details** ▾

System

IP Address

\* Operation

\* Upgrade Source

**Update Configuration Details** ▾

\* Select Protocol

Reset After Download ☐

Auto Commit ☐

Select patch(es) for update

The system displays the following error message when intermediate versions are unavailable in the selected **Upgrade Source** or Software Library:

Page contains error(s) - Software Version(s) <Version\_numbers> of Media Gateway must also be downloaded and present in the selected software library, <Software\_Library\_Name> for the selected upgrade path. Upgrading from <Older\_GatewayVersion> to <Later\_GatewayVersion> is a multi-step upgrade. Please see the Administering System Manager guide for more details.

If all required intermediate versions are present in the selected **Upgrade Source** software library, you can save the upgrade configuration and schedule the upgrade on the Upgrade Configuration page.

For viewing the multistep upgrades progress, you can click the **Upgrade Status** icon on the **Upgrade Management** page. To view **Job Status** and **Upgrade Path** steps with intermediate upgrades, if any, and their progress, click the **Upgrade Status** icon.

**Element Check Status**

**Upgrade Job Details** ✓ Passed ✗ Failed ⚠ Successful With Recommended or Patch Failure ⏸ Paused ❓ Not Started

**Detail Steps and Status for Avaya G430:HW1.0:V10** ✓

2 Items

| Step Name                         | Status | Start Time           | End Time             | Description |
|-----------------------------------|--------|----------------------|----------------------|-------------|
| Upgrading from 37.41.0 to 38.21.0 | ✓      | Aug 20, 2018 7:53 PM | Aug 20, 2018 7:59 PM |             |
| Upgrading from 38.21.0 to 39.5.0  | ✓      | Aug 20, 2018 7:59 PM | Aug 20, 2018 8:05 PM |             |

## Related links

[Configuring EASG during G430 Branch Gateway and G450 Branch Gateway upgrade](#) on page 1482

## Configuring EASG during G430 Branch Gateway and G450 Branch Gateway upgrade

### About this task

G430 Branch Gateway and G450 Branch Gateway support Enhanced Access Security Gateway (EASG) from version 39.5.0.

When G430 Branch Gateway or G450 Branch Gateway is upgraded to any version later than or same as 39.5.0, Solution Deployment Manager displays the **Enhanced Access Security Gateway (EASG)** field on the Edit Upgrade Configuration page.

To fetch the EASG configuration information, click **Refresh Element(s)**. Based on the **Refresh Element(s)** operation and the target upgrade version, the system displays the **Enhanced Access Security Gateway (EASG)** field.

If EASG is already enabled, the system does not prompt for the EASG configuration.

Use this procedure to configure EASG during the gateway upgrade.

### Procedure

1. On the **Edit Upgrade Configuration** page, do one of the following:
  - To enable EASG, type 1.
  - To disable EASG, type 2.

Auto Commit ☐

Select patch(es) for update

| Name                  | Location | Type | Version | CM Compatibility |
|-----------------------|----------|------|---------|------------------|
| No patches downloaded |          |      |         |                  |

Enhanced Access Security Gateway (EASG)

Enable: (Recommended)  
By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

Disable:  
By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG

End User License Agreement |

This field is mandatory.

If you leave it blank or type a value other than 1 or 2, the page displays the following error message.

Page contains error(s) - Please Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG.

2. Save the upgrade configuration.

3. To refresh the gateway after successful upgrade, click **Refresh Element(s)**.

Solution Deployment Manager does not prompt for EASG configuration in subsequent upgrades.

#### Related links

[G430 Branch Gateway and G450 Branch Gateway multistep upgrade overview](#) on page 1480

---

## Downloading a file

### About this task

Using **Download Manager**, you can download the software releases you are entitled from Avaya PLDS, or from an alternate source. You can upload a file from your local system to the software library using **Download Manager**.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the left navigation pane, click **Download Manager**.
3. From **Select Software/Hardware Types**, select the firmware you want to download.

You can choose either **Tree View** or **List View** to view the software, hardware types.

4. Click **Show Files**.

The system displays the upgrade files available for download. The system displays all the files for the category you selected. You can select only those files which you are entitled to.

5. Select a **Source** from where you want to download a software or firmware.
6. Select the files you want to download, and click **Download**.

The system displays the End User License Agreement page.

7. On the Library and Protocol Selection page, select a **Library** where you want to download the software or firmware.
8. On the Library and Protocol Selection page, select a **Protocol** through which you want to upload the downloaded software to the software library from System Manager. This scenario is applicable when the software library is on an external server.
9. Select the **I Agree** checkbox to download the software.

10. Perform one of the following actions:

- Click **Now** to download the software immediately.
- Click **Schedule** to schedule the download at a specified time.

To view the status of the download, click **Services > Scheduler** on the System Manager console.

To view the progress of the download, refresh the **File Download Status** section on the Download Manager page.

 **Note:**

- For IP Office upgrades, you must download the file to a remote HTTP software library. You can schedule an upgrade job only for a software library configured with an http URL.

The IP Office executable files are downloaded to the local System Manager repository and are available in the `$ABG_HOME/tools` folder.

- The system downloads the TN boards firmware files at home directory of the SCP user configured on the **SCP Configuration** tab of Remote SCP S/W Library irrespective of the path configured in the **Server Path** field on the **Library Server Details (L)** tab of the Add Software Library page.

---

## Upgrading Communication Manager 5.x

---

### Upgrading Communication Manager 5.x

#### Before you begin

Get the inventory for Communication Manager.

Analyze the software.

Download the software.

#### About this task

Use the procedure to upgrade Communication Manager 5.x to 5.2.1.

#### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. On the Software Inventory page, select the Communication Manager 5.x device that you want to upgrade.
6. Click **Upgrade**.
7. On the CM Upgrade Configuration page, perform the following:
  - a. Select the Communication Manager 5.2.1 device to which you want to upgrade.

- b. Provide the HTTP or HTTPS path for the EPW file.
- c. Browse and select the authentication file.
- d. In the Upgrade Operations section, complete the fields.
  - a. For semi automated upgrade, in the **Upgrade Source** field, select **Software Library**.
  - b. In the **Select Template** field, select a template.

For more information, see [CM Upgrade Configuration field descriptions](#) on page 1466.

- e. Click **Save the configuration**.
- 8. In the Job Schedule section, click **Now** or **Later**.
- 9. Click **Upgrade**.

The Software Inventory page displays the status of the upgrade in **Status**.

- 10. To view the logs and the description of the upgrade operation, click the status of the Communication Manager device.

#### Related links

[Analyze software](#) on page 1444

---

## Updating Communication Manager

### Procedure

- 1. On the System Manager web console, click **Services > Solution Deployment Manager**.
- 2. In the navigation pane, click **Upgrade Release Selection**.
- 3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
- 4. In the navigation pane, click **Upgrade Management > Software Inventory**.
- 5. On the Software Inventory page, select the Communication Manager you want to update.
- 6. Click **Upgrade**.
- 7. On the CM Upgrade Configuration page, select **Update** and fill in the required fields.
- 8. From the table, select the file you want to activate, deactivate, or remove.
- 9. In the Job Schedule section, click **Now** or **Later**.
- 10. Click **Upgrade**.

The Software Inventory page displays the status of the update in **Status**.

- 11. To view the logs and the description of the update, click the status of the Communication Manager device.

#### Related links

[Analyze software](#) on page 1444



---

## Updating the SAMP/MPC firmware

### Before you begin

- Add a Communication Manager system with the SAMP/MPC firmware to the System Manager inventory.
- Obtain the inventory and perform the analyze operation for Communication Manager.
- Download the appropriate SAMP/MPC firmware to the software library.

### About this task

You can only update SAMP/MPC firmware through the **Install (Copy and Unpack)/Update SAMP, MPC** option.

#### **Note:**

The procedure applies only to upgrading Communication Manager Release 5.x to 5.2.1.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Release Selection**.
3. In the **Upgrade to release** field, select **SMGR 6.3.8**, and click **Commit**.
4. In the navigation pane, click **Upgrade Management > Software Inventory**.
5. Click the Communication Manager that you want to update.
6. Perform the analyze operation.
7. Click **Upgrade**.
8. On the Patch Configuration page, click **Update**, and complete required fields.
9. Select the appropriate SAMP/MPC firmware from the table.
10. Click **Now** or **Schedule**.

---

## Protocol matrix for upgrades

**Table 10: Protocols supported by devices in Software Management**

| Product | Supported protocols | Notes                                                                                |
|---------|---------------------|--------------------------------------------------------------------------------------|
| G350    | FTP, USB            | Media modules associated with the gateway support the same protocols as the gateway. |

*Table continues...*



| Product               | Supported protocols                                  | Notes                                                                                                                |
|-----------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| G700                  | FTP                                                  | Media modules associated with the gateway support the same protocols as the gateway.                                 |
| G430                  | FTP, SCP (gateway versions later than 31.17.XX), USB | G430 supports the SCP protocol only if the current version of the gateway is 31.17.X or later.                       |
| G450                  | FTP, SCP (gateway versions later than 31.17.XX), USB | G450 supports the SCP protocol only if the current version of the gateway is 31.17.X or later.                       |
| G250                  | FTP, USB                                             | Media modules associated with the gateway support the same protocols as the gateway.                                 |
| TN Boards             | SCP                                                  | TN Boards support only the SCP protocol.                                                                             |
| Communication Manager | HTTP, HTTPS, SCP, FTP, SFTP                          | When you perform upgrades, use the protocols to copy the Communication Manager release files from the remote server. |
| System Manager        | HTTP, HTTPS, SCP, FTP, SFTP                          | When you perform upgrades, use the protocols to copy the System Manager release files from the remote server.        |

System Manager Solution Deployment Manager supports both FTP and SCP protocol supported remote library for Media gateway upgrade. This is strictly in accordance with the products and supported protocols in the above table.

For example, if a media gateway supports only FTP then you can only configure FTP protocol supported remote software library in System Manager Solution Deployment Manager Library management.

If a media gateway supports both SCP and FTP then you can configure either FTP or SCP protocol supported remote software library in the System Manager Solution Deployment Manager Library management.

#### Related links

[Analyze software](#) on page 1444

---

## Uploading the version.xml file

### About this task

Using **Upload Version XML**, you can upload the `version.xml` file from your local system to System Manager to perform upgrades.

### Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.

2. In the navigation pane, click **Upload Version XML**.
3. On the Upload Version XML page, click **Browse**.
4. Select the `version.xml` file from your local system and click **Open**.
5. Click **Commit** to upload the file.

The system displays the message: File upload is in progress. Please do not navigate away from this page.

# Chapter 24: Data Encryption

## Note:

From Release 8.1.2, System Manager supports the file system data encryption feature. This requires a new encryption capable variant of Release 8.1E OVA as prerequisite. The encryption can be enabled only at the time of deploying System Manager 8.1E OVA. Updating from System Manager 8.1 or 8.1.1 to System Manager 8.1.2 or later with files system encryption requires cold standby process.

From Release 8.1.2, you can enable or disable data encryption for Avaya Aura® applications at the time of deployment. Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment. Once you deploy the application with data encryption, you cannot disable data encryption after deployment.

By enabling Data Encryption, your Communication Product's certain Operational data and Log Files will be encrypted. You will be prompted to enter a passphrase that will be used to create or access an encryption key. You must remember the encryption passphrase, if not it can result in locking up the system. Secondly, you will be asked to configure the option for local key storage.

It is important to note that the encryption of the disk may have a performance impact. For further information, refer to the Avaya Product Administration guide(s). Before you select an encryption option, please read the Data Privacy Guideline so that you may better understand these options.

By disabling Data Encryption, your Communication Product's Operational data and Log Files will not be stored in encrypted partitions.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is selected, you need to reenter the encryption passphrase whenever the application reboots.

During reboot, the application prompts you to enter the encryption passphrase on VM console at first boot and upon entering the correct encryption passphrase, the system mounts all the encrypted disks.

Note the following:

- If a common encryption passphrase is used for all the encrypted partitions, but an incorrect encryption passphrase is entered in first attempt, then you have to enter the correct encryption passphrase for every partition at least once.
- Multiple failures on encryption passphrase boots the system into the Maintenance/Emergency mode. To get the prompt again, you need to reboot the system.

If encryption is enabled and the **Require Encryption Pass-Phrase at Boot-Time** check box is not selected during OVA deployment, the application creates the Local Key Store and the system does

not prompt you to type the encryption passphrase whenever the application reboots to mount the encrypted disks. You can also set up the remote key server by using the **encryptionRemoteKey** command after the deployment of the application.

### Encryption of System Manager partitions

When you enable data encryption for System Manager, the system encrypts the following partitions that have personal data.

- /var/log
- /var/log/audit
- /var/lib/pgsql/data
- /var/opt/nortel/cnd

---

## Remote Key Server

When you enable data encryption for an application, you can set up remote key server. You can add multiple remote key servers. When you add a remote key server for the first time, the application disables the local key store. You can enable the local key store again after adding a remote key server. However, it is not recommended to enable local key store when the remote key server configuration exists.

If there is only one empty slot, then you cannot add a new remote key server or a new passphrase. The last empty slot is a “reserved” slot and you can use that only for changing the passphrase.

Application checks for the remote key server accessibility every 15 minutes. If any of the remote key server goes down, the application generates a Warning alarm. If all remote key servers are not accessible, then the application generates a Minor alarm.

---

## Data Encryption password policy

The encryption passphrase must meet the following requirements:

- Must contain at least eight characters.
- Must contain at least one of each: an uppercase letter, a lowercase letter, a numerical, and a special character.

Ensure that you keep the encryption passphrase safe. You need the encryption passphrase later.

---

## Data encryption commands

The following CLI commands are available to make changes to the data encryption settings.

---

### encryptionPassphrase command

Using the **encryptionPassphrase** command you can manage the encryption passphrase after deploying the application.

#### Syntax

```
encryptionPassphrase [add | change | remove | list]
```

- |               |                                                           |
|---------------|-----------------------------------------------------------|
| <b>add</b>    | Displays the prompts to add the encryption passphrase.    |
| <b>change</b> | Displays the prompts to change the encryption passphrase. |
| <b>remove</b> | Removes the encryption passphrase.                        |
| <b>list</b>   | Displays the encryption passphrase and slot assignment.   |

#### Considerations

You must deploy the application with data encryption.

### Adding encryption passphrase

#### About this task

Use the **encryptionPassphrase add** command to add encryption passphrase.

You can add a maximum of seven encryption passphrases, if free slots are available.

#### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase add**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. In **Enter existing passphrase**, type the encryption passphrase.
5. In **Enter new Passphrase**, type the new encryption passphrase.
6. In **Retype Passphrase**, retype the encryption passphrase.

### Changing encryption passphrase

#### About this task

Use the **encryptionPassphrase change** command to change the existing encryption passphrase.

## Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase change**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. At the prompt, in **Current Passphrase**, type the encryption passphrase.
5. In **Enter new Passphrase**, type the new encryption passphrase.
6. In **Retype Passphrase**, retype the encryption passphrase.

The application displays the following message.

```
Passphrase successfully changed.
```

## Displaying encryption passphrase and slot assignment

### About this task

Use the **encryptionPassphrase list** command to list the slots assignment, encryption passphrase, and remote server details.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase list**.
3. When the system prompts for privileged command execution verification [sudo], type the password.

The application displays the details based on the system configuration.

| Slot        | Status   | Passphrase/Remote Server |
|-------------|----------|--------------------------|
| Key Slot 0: | ENABLED  | Passphrase               |
| Key Slot 1: | ENABLED  | Passphrase               |
| Key Slot 2: | ENABLED  | Passphrase               |
| Key Slot 3: | DISABLED | empty                    |
| Key Slot 4: | DISABLED | empty                    |
| Key Slot 5: | DISABLED | empty                    |
| Key Slot 6: | DISABLED | empty                    |
| Key Slot 7: | DISABLED | empty                    |

## Removing encryption passphrase

### About this task

Use the **encryptionPassphrase remove** command to remove the existing encryption passphrase. You cannot remove all encryption passphrases, the application retains minimum one encryption passphrase.

If you attempt to delete the last encryption passphrase, the system displays the following message:

```
The last passphrase cannot be removed!
```

## Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionPassphrase remove**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. At the prompt, in **Passphrase to remove**, type the existing encryption passphrase.

The application displays the following message.

```
Passphrase successfully removed.
```

---

## encryptionRemoteKey command

Using the **encryptionRemoteKey** command you can manage the remote key server after deploying the application.

### Syntax

```
encryptionRemoteKey [add | remove | list]
```

- |               |                                                     |
|---------------|-----------------------------------------------------|
| <b>add</b>    | Displays the prompts to add the remote key server.  |
| <b>remove</b> | Removes the remote key server.                      |
| <b>list</b>   | Displays the remote key server and slot assignment. |

### Considerations

You must deploy the application with data encryption.

## Adding remote key server

### Before you begin

Ensure that the remote key server is configured and accessible.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey add** <Address> <Port>.

Where:

**Address** is the IP address or FQDN of the remote key server.

**Port** is the port number of the remote key server. If you do not enter the port number the application uses the value of default port as 80.

3. When the system prompts for privileged command execution verification [sudo], type the password.

4. In **Enter existing passphrase**, type the existing encryption passphrase.

If the remote key server is not configured, the application displays the following message.

```
Remote key server not found
```

If the remote key server is configured, the application adds the remote key server. When you add a remote key server for the first time, the application disables the local key store.

## Removing remote key server

### About this task

Use the **encryptionRemoteKey remove** command to remove the existing remote key server.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey remove** <Address>.

Where:

**Address** is the IP address or FQDN of the remote key server.

You must use the same IP address or FQDN value that you used to add the remote key server.

3. When the system prompts for privileged command execution verification [sudo], type the password.
4. In **Passphrase**, type the existing encryption passphrase.

The application removes the remote key server and displays the following message:

```
RemoteKey successfully removed.
```

## Displaying remote key server and slot assignment

### About this task

Use the **encryptionRemoteKey list** command to list the slots assignment, encryption passphrase, and remote server details.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionRemoteKey list**.
3. When the system prompts for privileged command execution verification [sudo], type the password.

The application displays the details based on the system configuration.

| Slot        | Status  | Passphrase/Remote Server          |
|-------------|---------|-----------------------------------|
| Key Slot 0: | ENABLED | Passphrase                        |
| Key Slot 1: | ENABLED | <IP Address of Remote Key Server> |
| Key Slot 2: | ENABLED | Passphrase                        |



```
Key Slot 3: DISABLED empty
Key Slot 4: DISABLED empty
Key Slot 5: DISABLED empty
Key Slot 6: DISABLED empty
Key Slot 7: DISABLED empty
```

## encryptionLocalKey command

Using the **encryptionLocalKey** command you can enable or disable the local key store after deploying the application with data encryption.

### Syntax

```
encryptionLocalKey [enable | disable]
```

**enable**                      Enables the local key store.

**disable**                     Disables the local key store.

### Considerations

You must deploy the application with data encryption.

## Enabling local key store

### About this task

Use the **encryptionLocalKey enable** command to enable the local key store.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey enable**.
3. When the system prompts for privileged command execution verification [sudo], type the password.
4. At the prompt, in **Enter existing passphrase**, type the existing encryption passphrase.

If the local key store is already enabled, the application displays the following message.

```
Local key store is already enabled.
```

## Disabling local key store

### About this task

Use the **encryptionLocalKey disable** command to disable the local key store.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type **encryptionLocalKey disable**.

3. When the system prompts for privileged command execution verification [sudo], type the password.

The application displays the following message.

```
Local keystore removed
```

```
Local Key Store is now disabled.
```

---

## Viewing data encryption status

### About this task

The **encryptionStatus** command displays information about encryption on the system.

### Procedure

1. Log in to the application command line interface with administrator privileged credentials.
2. Type `encryptionStatus`.
3. When the system prompts, type the password.

For example, if the local key store is configured, the system displays the following status:

```
Data Encryption: enabled
Number of PassPhrases used: <n>
Local Key Store: enabled
Encryption Passphrase Required at Boot-time: no
```

For example, if the remote key server is configured, the system displays the following status:

```
Data Encryption: enabled
Local Key Store: disabled
Encryption Passphrase Required at Boot-time: yes
remoteKeyServers: <remoteServer1: <remoteServerIPAddress> accessible>
```

# Chapter 25: Communication Manager Notify Sync

---

## Communication Manager notify synchronization

When you perform an administrative task from System Manager, the local database is immediately updated. If you do the action through a Communication Manager SAT screen, or through a phone, or from any of the several management applications such as Site Administration, MultiSite Administration, Native Configuration Manager, or MyPhone, it is not immediately reflected in System Manager. This scenario creates an out-of-sync condition between the Communication Manager and System Manager.

The CM notify sync feature provides:

- Near-real time notifications from Communication Manager to System Manager whenever you run certain tasks against a Communication Manager object from a system other than System Manager
- Notifications whenever the tti-m, tti-s, psa-u, psa-a, or psa-d login perform predefined actions against a Communication Manager station object.

After a Communication Manager sends notifications to System Manager, System Manager discovers the complete details of the task you performed. The transmission of notifications in the form of event messages from Communication Manager to System Manager is based on the existing rsyslog capability of Communication Manager. rsyslog uses UDP or TCP to send event messages from the originating Communication Manager to the System Manager.

### **Note:**

The daily default synchronization and any other scheduled synchronization operations are unaffected by the CM notify sync feature.

You need Communication Manager 6.2 or later to enable the CM notify sync feature. System Manager 6.3 supports one-way and two-way TLS.

### **Enable the CM notify sync feature**

You can enable and disable the CM notify sync feature on each Communication Manager. You can activate the CM notify sync feature from **Manage Elements** of a new System Manager. Select Communication Manager 6.2 or later, and select **Enable Notifications** in the Attributes section.

As a system administrator, you must specify the IP addresses of one or two System Manager servers to which Communication Manager sends the event data using rsyslog. If your

configuration includes two System Manager servers, the standby System Manager ignores the syslog messages until the System Manager becomes active.

## Configuring one-way and two-way TLS

You must configure one-way or two-way TLS for the CM notify sync feature.

To configure one-way TLS, perform the following:

- [Downloading the System Manager PEM certificate](#) on page 153
- [Downloading the pem file to Communication Manager](#) on page 1499
- [Adding a trusted certificate to Communication Manager](#) on page 1500
- [Configuring notify sync between Communication Manager and System Manager](#) on page 1501

### **Note:**

You must add the Communication Manager in **Inventory > Manage Elements** before enabling the notify sync feature on the Communication Manager. If you add the Communication Manager in the System Manager **Inventory**, and enable notify sync before adding the certificate, add the trusted certificate to the Communication Manager. Then edit the Communication Manager through **Manage Elements**, and re-enable the Communication Manager notify sync feature.

To configure two-way TLS, do the following:

- [Downloading the System Manager PEM certificate](#) on page 153
- [Downloading the pem file to Communication Manager](#) on page 1499
- [Adding a trusted certificate to Communication Manager](#) on page 1500
- [Configuring notify sync between Communication Manager and System Manager](#) on page 1501
- [Adding the Communication Manager certificate to the System Manager trust](#) on page 1503
- [Enabling two-way TLS in System Manager](#) on page 1504

---

## Downloading the System Manager PEM certificate

### Procedure

1. On the System Manager web console, click **Services > Security**.
2. In the navigation pane, click **Certificates > Authority**.
3. Click **CA Functions > CA Structure & CRLs**.
4. Click **Download PEM file**.

The system downloads the .pem file on your system.

### Related links

[Exchanging CA certificates between System Manager and Avaya Meetings Management](#) on page 152

# Downloading the pem file to Communication Manager

## Procedure

1. Log in to a Communication Manager web console.
2. Click **Administrator > Server (Maintenance)**.
3. In the left navigation pane, click **Miscellaneous > Download Files**.
4. Select the **Files to download from the machine I'm using to connect to the server** option.
5. Click **Choose File** to browse to the downloaded certificate.
6. Click **Download**.

The system displays the Download Files Results page with a message that the download is successful.

## Download Files

The Download Files SMI page lets you download files to the server.

☒ File(s) to download from the machine I'm using to connect to the server

No file chosen

No file chosen

No file chosen

No file chosen

☐ File(s) to download from the LAN using URL


Proxy Server  (e.g proxy.domain:3152)

---

## Adding a trusted certificate to Communication Manager

### Procedure

1. Log in to a Communication Manager Web console.
2. Click **Administration > Server (Maintenance)**
3. Click **Security > Trusted Certificates**.
4. Click **Add**.
5. On the Trusted Certificate – Add page enter the file name for the certificate you want to add. The certificate must be a .pem file. The name of the certificate must be the same as the one used in the Downloading the pem file to Communication Manager section.
6. To validate the certificate, click **Open**.

After a successful validation, the Trusted Certificates – Add page displays the **issued-to**, **issued by**, and **expiration date** information for the certificate you are adding.

 **Note:**

The system displays an error message if the certificate is not a valid certificate.

7. Select the **Communication Manager, Remote Logging** repositories from the list of trusted repositories.
8. Click **Add**.

The system verifies the following:

- The certificate name has a .crt extension. If the certificate name has a different extension, the system deletes it and replaces it with a .crt extension.
- The certificate name is unique and does not already exist.
- The certificate is not a duplicate certificate with a new name.

## Trusted Certificates

This page provides management of the trusted security certificates present on this server.

[Add this certificate](#)

Issued To Issued By Expiration Date

default default Sat Dec 18 2021

smgr-99.crt

Store the certificate in this file in each repository selected below

[Add to these trusted repositories](#)

- ☐ Authentication, Authorization and Accounting Services (e.g. LDAP)
- ☒ Communication Manager
- ☐ Web Server
- ☒ Remote Logging

**Add** **Cancel** **Help**

## Configuring notify sync between Communication Manager and System Manager

### About this task

When Geographic Redundancy is configured, on Communication Manager, the system registers the IP address of the primary or secondary System Manager that manages Communication Manager.

### Before you begin

On the Manage Elements page, register both the IP addresses of the duplex Communication Manager pair for System Manager to handle the notify sync messages.

### \* Note:

In a duplex configuration, you cannot use the virtual address on Communication Manager.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select a Communication Manager system.
4. In the Attributes section, select **Enable Notifications**.

When you enable notify sync, the system sends a register command to Communication Manager for registering the IP address of System Manager as a syslog server. The system sends all administrative changes that you make on Communication Manager to System Manager.

5. To verify that the notify sync feature is successfully enabled, do the following:
  - a. Using an SSH client, log in to Communication Manager as sroot.
  - b. At the prompt, type `sudo /opt/ws/cmSyslogConfig --iptcmquery`.

The system displays the details of the registration.

6. When the notify sync is nonoperational, and when Geographic Redundancy is set up on System Manager, complete the following:
  - a. Ensure that you have root permissions to Communication Manager to edit the file.
  - b. Using an SSH client, log in to Communication Manager as root.
  - c. Open the `/etc/syslog.conf` file.

- d. Add hash (#) at the beginning of the following secondary System Manager related entries in the file:

```
$ActionSendStreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode x509/certvalid
#local6.* @[148.147.162.36]:9000
```

- e. To restart the rsyslog service on Communication Manager, type `service rsyslog restart`.

Notify sync becomes operational.

7. If the primary System Manager becomes nonoperational, and you want to manage Communication Manager by using the secondary System Manager, complete the following:
  - a. In the `/etc/syslog.conf` file, replace the primary System Manager IP address with the secondary System Manager IP address.

```
iptcm_log local6.*
$DefaultNetstreamDriverCAFile /etc/opt/ecs/certs/rsyslog/CA/all-ca.crt
$ActionSendStreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode x509/certvalid
#local6.* @[148.147.162.36]:9000
```

- b. Remove hash (#) at the beginning of the following secondary System Manager related entries in the file:

```
$ActionSendStreamDriver gtls
$ActionSendStreamDriverMode 1
$ActionSendStreamDriverAuthMode x509/certvalid
local6.* @[148.147.162.35]:9000
```



---

## Configure two-way TLS

You must configure either one-way or two-way TLS to enable the Communication Manager notification service. To configure two-way TLS, do the following:

- [Downloading the System Manager PEM certificate](#) on page 153
- [Downloading the pem file to Communication Manager](#) on page 1499
- [Adding a trusted certificate to Communication Manager](#) on page 1500
- [Configuring notify sync between Communication Manager and System Manager](#) on page 1501
- [Adding the Communication Manager certificate to the System Manager trust](#) on page 1503
- [Enabling two-way TLS in System Manager](#) on page 1504

---

## Adding the Communication Manager certificate to the System Manager trust

### Before you begin

1. Download the System Manager certificate.
2. Download the pem file to Communication Manager.
3. Add a trusted certificate to the Communication Manager.
4. Configure notify sync on the Communication Manager.

### Procedure

1. Download the Communication Manager certificate to your computer from `/etc/opt/ecs/certs/rsyslog/CA/sip_product_root.crt`.
2. Log on to System Manager Web Console.
3. On the System Manager web console, click **Services > Inventory**.
4. In the navigation pane, click **Manage Elements**.
5. Select **System Manager** from the elements list.
6. Click **More Options > Manage Trusted Certificates**.
7. Click **Add**.
8. In the **Select Store Type to add trusted certificate** field, select **TM\_INBOUND\_TLS** as the store type.
9. Click **Import from file**.
10. Click **Choose File**.

11. Browse to the certificate that you have downloaded, and click **Open**.
12. Click **Retrieve certificate** to check the contents of the certificate.
13. Review the certificate details, and click **Commit**.

---

## Enabling two-way TLS in System Manager

### Before you begin

Add the Communication Manager certificate to the System Manager trust.

### About this task

Perform the following procedure during off peak hours or during a planned outage since you have to restart the JBoss service after enabling two-way TLS.

### Procedure

1. Login to the System Manager CLI using the admin credentials.
2. Browse to the `$IPTCM_HOME/config/workflow` folder and open the `notify-sync.properties` file for editing.
3. In the `iptcm.authtype.twowaytls` property, change the value to **`iptcm.authtype.twowaytls=true`**.

The default value is **`iptcm.authtype.twowaytls=false`**.

4. Restart the System Manager JBoss service using the **`service jboss restart`** command.

# Chapter 26: System Manager Network Configuration

---

## Out of Band Management in System Manager

Out of Band Management is two physically or logically separated network connections or both that connects to a private management network of the customer. The network connection provides secure management and administration of Avaya products. With Out of Band Management, you can separate the management network and data network traffic to System Manager.

System Manager provides the following network interfaces:

- The regular eth0 interface that was present in releases earlier than System Manager Release 8.1.3, is called the Management interface or Out of Band Management interface. The IP address is called as the Management IP address. The Management interface is mandatory for configuration.

The following are the examples of System Manager Management network traffic:

- Database replication with Session Manager
- Element management. For example, Session Manager, Communication Manager, and Avaya Breeze® platform.
- User management
- Solution deployment, upgrades, and software patch install
- If Out of Band Management is enabled, then the public interface is configured with Public IP address and used for the nonmanagement traffic. This is an optional configuration.

The following are the examples of System Manager nonmanagement or public network traffic:

- End-user self-provisioning
- Client devices getting certificates through SCEP
- Tenant Management

Out of Band Management configuration persists across System Manager upgrades, updates, and restarts.

For configuring Out of Band Management in System Manager, System Manager must be installed on an Appliance Virtualization Platform host that is configured with Out of Band Management. Out of Band Management is enabled during the deployment of Appliance Virtualization Platform.

**\* Note:**

Once OOBM is enabled on System Manager, public interface eth1 is no longer reachable using ping command from other systems that are present in a public network. However, System Manager can reach other systems on a public interface.

**Out of Band Management in a Geographic Redundancy setup**

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

**Restoring System Manager backup**

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.

**Tenant Management on Out of Band Management-enabled System Manager**

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

---

## Configuring Out of Band Management on System Manager

**About this task**

If you do not configure Out of Band Management during the deployment of System Manager OVA from Solution Deployment Manager on an Avaya-provided server, you can use the `configureOOBM` command to configure Out of Band Management anytime after the deployment.

**Before you begin**

- Enable Out of Band Management on Appliance Virtualization Platform.
- Install System Manager on the Appliance Virtualization Platform host on which Out of Band Management is installed.
- Ensure that IP address or hostname of Public network and Management network are different.

If both are in the same network, Out of Band Management configuration might not function as expected.

- Log in to System Manager by using an SSH client utility.

When you enable Out of Band Management configuration, you might lose the connection as the system does a network restart. You can login to System Manager from the Console of VMware vSphere Web Client. that is configured to connect to the Appliance Virtualization Platform host server.

## Procedure

1. To enable Out of Band Management, type `configureOOBM -EnableOOBM`.

The system enables Out of Band Management on the System Manager virtual machine. With **EnableOOBM**, the system configures the additional Ethernet interface, updates network configuration, and sets the firewall rules.

2. To disable Out of Band Management, type `configureOOBM -DisableOOBM`.

The system disables Out of Band Management on the System Manager virtual machine. With **DisableOOBM**, the system disables the additional Ethernet interface that you configured earlier and sets the firewall rules to default.

---

# Configuring Out of Band Management on System Manager in the Geographic Redundancy setup

## About this task

### Note:

You cannot enable Out of Band Management on secondary System Manager server when Out of Band Management on primary System Manager server is disabled.

## Before you begin

Identify one of the following:

- Enable Out of Band Management on both the primary and secondary System Manager server.
- Enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on the secondary System Manager server.
- Disable Out of Band Management on secondary System Manager server.
- Disable Out of Band Management on both the primary and secondary System Manager server.

## Procedure

1. To enable Out of Band Management on both primary and secondary System Manager server, perform the following:
  - a. Disable Geographic Redundancy replication on primary System Manager server.
  - b. Convert primary System Manager server to standalone System Manager server and activate the secondary System Manager server.
  - c. Enable Out of Band Management on both primary and secondary System Manager server.
  - d. Reconfigure the Geographic Redundancy on the secondary System Manager server.

- e. Enable Geographic Redundancy replication on primary System Manager server.
2. To enable Out of Band Management on the primary System Manager server and not enable Out of Band Management on secondary System Manager server, perform the following:
  - a. Disable Geographic Redundancy replication on primary System Manager server.
  - b. Convert primary System Manager server to standalone System Manager server.
  - c. Enable Out of Band Management on primary System Manager server.
  - d. Once Out of Band Management on primary System Manager server is enabled, reconfigure Geographic Redundancy on secondary System Manager server.
  - e. Enable Geographic Redundancy replication on primary System Manager server.
3. To disable Out of Band Management on secondary server, perform the following:
  - a. Disable Geographic Redundancy replication on primary System Manager server.
  - b. Convert primary System Manager server to standalone System Manager server.
  - c. Activate secondary System Manager server and disable Out of Band Management.
  - d. Reconfigure primary System Manager server from the web console of the secondary System Manager server.
  - e. Enable Geographic Redundancy replication on primary System Manager server.
4. To disable Out of Band Management on both servers, perform the following:
  - a. Disable Geographic Redundancy replication on primary System Manager server.
  - b. Convert primary System Manager server to standalone System Manager server and disable Out of Band Management.
  - c. Activate secondary System Manager server and disable Out of Band Management.
  - d. Reconfigure Geographic Redundancy on secondary System Manager server with old primary System Manager server which is now standalone.
  - e. Enable Geographic Redundancy replication on primary System Manager server.

---

## Changing the IP address and FQDN in System Manager

---

### Impact of change in FQDN and IP address on the Geographic Redundancy feature

In a Geographic Redundancy configuration, the system automatically communicates any change in the IP address or FQDN of the primary or the secondary System Manager to the elements.

**Impact of the change in IP address or FQDN on the primary System Manager**

- The system changes the identity certificates of the primary System Manager. Therefore, reinitialize trust on the primary System Manager.
- The secondary System Manager does not require any trust changes.
- System Manager notifies the change to the elements. If the event notification fails due to temporary disconnect, the system sends the event when the elements resume the network connectivity.

**Impact of the change in IP address or FQDN on the secondary System Manager in the active and stand-by mode**

- The system changes the identity certificates of the secondary System Manager. Therefore, reinitialize trust on the secondary System Manager.
- The primary System Manager does not require any trust changes.
- System Manager notifies the change to the elements. If the event notification fails due to temporary disconnect, the system sends the event when the elements resume the network connectivity.

**Impact of the change in IP address or FQDN during a network split**

When the split network heals, run the IPFQDN pair.

---

## **SSO login to remote machine fails**

For System Manager deployments that involve remote machines such as CS 1000 servers and solutions based on the System Manager Single Sign On (SSO) client, SSO between System Manager and the remote machine fails.

During the data migration or IP-FQDN change, the system does not import the LDAP attribute that contains the SSO cookie domain value back to the directory. Therefore, the System Manager SSO login to the remote machine fails. You must enable SSO after the data migration or the IP-FQDN change.

**Related links**

[Reimporting the SSO cookie domain value](#) on page 75

---

## **Changing network parameters on System Manager**

**Changing the IP address, FQDN, DNS, Gateway, or Netmask address of System Manager from CLI****About this task**

Use this procedure to change the network configuration parameters for Public interface and Management interface when OOBM is enabled.

**! Important:**

- Do not change the network settings from vSphere Web Client when the virtual machine is in the power off state.
- FQDN value must be unique and different from the virtual FQDN value of System Manager.

**Before you begin**

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.
- Create the System Manager virtual machine snapshot.

**\* Note:**

Delete the snapshot after the System Manager operation is complete.

**Procedure**

1. To configure Management network parameters, type `changeIPFQDN -IP <IPv4 address> -FQDN <FQDN> -GATEWAY <Gateway IPv4 address> -NETMASK <Netmask address> -DNS <DNS address> -SEARCH <search list of domain names> -IPV6 <IPv6 address> -IPV6GW <IPv6 Gateway address> -IPV6PREFIX <IPv6 prefix>.`

For information, see **changeIPFQDN**.

2. To configure Public network parameters, type `changePublicIPFQDN -IP <IP address> -PublicFQDN <FQDN> -PublicGATEWAY <Gateway IP address> -PublicNETMASK <Netmask address>.`

For information, see **changePublicIPFQDN**.

**Next steps**

Get new licenses from PLDS containing the new host ID and install the new licenses.

After you change the IP address of System Manager, the system generates a new host ID for WebLM server that System Manager hosts. Therefore, all previously installed licenses become invalid.

For instructions to install a license file, see Managing Licenses in *Administering Avaya Aura® System Manager*.

**Related links**

[System Manager command line interface operations](#) on page 1518

[changeIPFQDN command](#) on page 1510

**changeIPFQDN command**

Use the **changeIPFQDN** command to change the Management IP address when Out of Band Management is enabled. With this command you can change the IP address, FQDN, DNS



address, Gateway, Netmask address for Management network configuration of System Manager, and the search list for the DNS address.

**\* Note:**

On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the **changeIPFQDN** command, the system changes the host ID of System Manager and invalidate the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.

To change the Public IP address when Out of Band Management is enabled, use the **changePublicIPFQDN** command

## Syntax

```
changeIPFQDN -IP < > -FQDN < > -GATEWAY < > -NETMASK < > -DNS < > -SEARCH < > -IPV6 < > -IPV6GW < > -IPV6PREFIX < >
```

| # | Option     | Description                                                                                                                    | Usage                                                                                |
|---|------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 1 | IP         | The new Management IPv4 address of System Manager.                                                                             | <b>changeIPFQDN -IP 10.11.12.13</b>                                                  |
| 2 | FQDN       | The new Management FQDN of System Manager.                                                                                     | <b>changeIPFQDN -FQDN a.mydomain.smgr.com</b>                                        |
| 3 | GATEWAY    | The new Management Gateway IPv4 address of System Manager.                                                                     | <b>changeIPFQDN -GATEWAY 10.11.1.1</b>                                               |
| 4 | NETMASK    | The new Management netmask address of System Manager.                                                                          | <b>changeIPFQDN -NETMASK 255.255.203.0</b>                                           |
| 5 | DNS        | The new Management DNS address of System Manager.<br>You can provide multiple DNS addresses. Separate each address by a comma. | <b>changeIPFQDN -DNS 10.11.1.2</b><br><b>changeIPFQDN -DNS 10.11.12.5,10.11.12.3</b> |
| 6 | SEARCH     | The new search list of domain names.                                                                                           | <b>changeIPFQDN -SEARCH smgr.com</b>                                                 |
| 7 | IPV6       | The new Management IPv6 address of System Manager.                                                                             | <b>changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080</b>                    |
| 8 | IPV6GW     | The new Management Gateway IPv6 address of System Manager.                                                                     | <b>changeIPFQDN -IPV6GW 2001:b00d::1</b>                                             |
| 9 | IPV6PREFIX | The new Management netmask prefix of System Manager. The default value is 64.                                                  | <b>changeIPFQDN -IPV6PREFIX 64</b>                                                   |

## Example

You can provide options in any combination that the system supports:

```
changeIPFQDN -IP 10.11.y.z -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1 -NETMASK 255.255.255.0 -DNS 10.11.1.2 -SEARCH platform.avaya.com
```

```
changeIPFQDN -FQDN a.domain.weblm.com -GATEWAY 10.11.1.1
```

```
changeIPFQDN -IP 10.11.y.z
```

```
changeIPFQDN -IPV6 2001:b00d:dead:1111:1111:1111:1234:8080 -IPV6GW 2001:b00d::1 -IPV6PREFIX 64
```

## Changing IP address or FQDN of managed elements

### About this task

For instructions to change the IP address or FQDN of managed elements, see the application-specific document. For example, for Session Manager, see *Maintaining and Troubleshooting Avaya Aura® Session Manager*.

### Procedure

1. On the System Manager web console, click **Services > Inventory**.
2. In the navigation pane, click **Manage Elements**.
3. Select the registered element from the table.
4. Click **Edit**.
5. In the **General** section, in the **Node** field, type the appropriate value.
6. In the **Access Profile** section, in the **Host** field, type the appropriate value.

## Changing the System Manager IP address in managed elements

### About this task

When the IP address or FQDN of System Manager changes:

- If the managed elements use JNDI lookup to communicate with System Manager, the elements must point to the new System Manager IP address.
- The adopting element must recreate the License Manager object with the new IP address.
- Data replication on managed elements, such as Session Manager and Presence can have an impact because both elements use the System Manager host name to communicate with System Manager.

Therefore, you must change the references of System Manager IP address and FQDN on the managed elements, such as Session Manager, Presence, and AES so the elements can continue to connect and communicate with System Manager.

## Procedure

To change the IP address or FQDN of System Manager on the managed elements, see the documentation of the element.

For example, to change the IP address or FQDN of System Manager on Session Manager, see *Maintaining and Troubleshooting Avaya Aura® Session Manager* on the Avaya support site.

---

# Changing the IP address and FQDN on the System Manager servers in Geographic Redundancy

---

## Change in IP address and FQDN on the primary and secondary System Manager servers

The sections provide various scenarios for changing the IP address and FQDN on System Manager configured with Geographic Redundancy. The section also provides the procedure to run the pair IP-FQDN script.

Ensure that the IP address and FQDN meets the following requirements:

- For the IP address change: Map the new IP address of the FQDN of System Manager in DNS.

Ensure that the new IP address is unique.

- For the FQDN change: Map the new FQDN to the IP address of System Manager in DNS.

Ensure that the new FQDN is unique and different from the virtual FQDN.

- For the IP address and FQDN change: Ensure that the new IP address and FQDN is valid and mapped in DNS.

### Note:

Entering an invalid IP address and FQDN might affect the behavior of the system.

---

## Changing the IP address and FQDN on the primary System Manager when the secondary is in the standby or active mode

### Procedure

1. Disable the Geographic Redundancy replication if not already disabled.
2. On the primary System Manager server, change the IP address or FQDN or both. For instructions, see *Changing the IP address and FQDN in System Manager*.

Wait for about 30–40 minutes before you perform the next step.

3. Log on to the web console of the primary System Manager server, and verify that System Manager is up and running.
4. Log in to the CLI of the secondary System Manager server with administrator privilege CLI user credentials and perform one of the following:
  - If you changed both the IP address and FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server> -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>
```
  - If you changed the IP address, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server>
```
  - If you changed FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>
```
5. On the secondary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the primary System Manager server.
6. Enable the Geographic Redundancy replication.

#### Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Disabling the Geographic Redundancy replication](#) on page 112

---

## Changing the IP address and FQDN on the primary System Manager server when the secondary is nonoperational

### Procedure

1. Disable the Geographic Redundancy replication if not already disabled.
2. On the primary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.  
Wait for about 30–40 minutes before you perform the next step.
3. Log on to the web console of the primary System Manager server, and verify that System Manager is up and running.
4. Bring the secondary System Manager server to operation.
5. Log in to the CLI of the secondary System Manager server with administrator privilege CLI user credentials and perform one of the following:
  - If you changed both the IP address and FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server> -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>
```

- If you changed the IP address, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the primary server> -NEWIP <New IP of the primary server>
```

- If you changed FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of the primary server> -NEWFQDN <New FQDN of the primary server>
```

6. On the secondary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the primary System Manager server.
7. Enable the Geographic Redundancy replication.

#### Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Disabling the Geographic Redundancy replication](#) on page 112

---

## Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode

### Procedure

1. Disable the Geographic Redundancy replication if not already disabled.
2. On the secondary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.

Wait for about 30–40 minutes before you perform the next step.

3. Log on to the web console of the secondary System Manager server, and verify that System Manager is running.
4. Log in to the CLI of the primary System Manager server with administrator privilege CLI user credentials and perform one of the following:

- If you changed both the IP address and FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the secondary server> -NEWIP <New IP of the secondary server> -OLDFQDN <Old FQDN of the secondary server> -NEWFQDN <New FQDN of the secondary server>
```

- If you changed the IP address, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the secondary server> -NEWIP <New IP of the secondary server>
```

- If you changed FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN <Old FQDN of the secondary server> -NEWFQDN <New FQDN of the secondary server>
```

5. On the primary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the secondary System Manager server.
6. Enable the Geographic Redundancy replication.

#### Related links

[Enabling the Geographic Redundancy replication](#) on page 111

[Disabling the Geographic Redundancy replication](#) on page 112

---

## Changing the IP address and FQDN on the secondary System Manager server when the primary is nonoperational

### Procedure

1. On the secondary System Manager server, change the IP address or FQDN or both. For instructions, see Changing the IP address and FQDN in System Manager.

Wait for about 30–40 minutes before you perform the next step.

2. Log on to the web console of the secondary System Manager server, and verify that System Manager is running.
3. Bring the primary System Manager server to operation.
4. Log on to the primary System Manager server and disable the Geographic Redundancy replication if not already disabled.
5. On the primary System Manager server, verify that the Geographic Redundancy page displays the new IP address or FQDN of the secondary System Manager server.
6. Log in to the CLI of the primary System Manager server with administrator privilege CLI user credentials and perform one of the following:

- If you changed both the IP address and FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old IP of the secondary server> -NEWIP <New IP of the secondary server> -OLDFQDN <Old FQDN of the secondary server> -NEWFQDN <New FQDN of the secondary server>
```

- If you changed the IP address, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDIP <Old
IP of the secondary server> -NEWIP <New IP of the secondary
server>
```

- If you changed FQDN, type the following:

```
#sh $MGMT_HOME/utils/ipfqdnchange/pairIpFqdnChange.sh -OLDFQDN
<Old FQDN of the secondary server> -NEWFQDN <New FQDN of the
secondary server>
```

## System Manager command line interface operations

| # | Command      | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Usage                                                                                                                                                                                                                                                                                                                                                  |
|---|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | changeIPFQDN | <ul style="list-style-type: none"> <li>• -IP &lt;new Management interface or Out of Band Management IP address for System Manager&gt;</li> <li>• -FQDN &lt;new Management or Out of Band Management fully qualified domain name for System Manager&gt;</li> <li>• -GATEWAY &lt;new Management interface or Out of Band Management Gateway address for System Manager&gt;</li> <li>• -NETMASK &lt;new Management interface or Out of Band Management netmask address for System Manager&gt;</li> <li>• -DNS &lt;new DNS address for System Manager&gt;</li> <li>• -SEARCH &lt;new search list for DNS address&gt;</li> </ul> | <p>Updates the existing Management interface or Out of Band Management IP address, FQDN, Gateway, Netmask, DNS, and the search list with the new value.</p> <p><b>* Note:</b></p> <p>On the System Manager Release 7.1 and later system, if you change the IP Address of System Manager by using the <b>changeIPFQDN</b> command, the system changes the host ID of System Manager and invalidate the existing installed license file. Therefore, you must reinstall the license file on System Manager after changing the IP Address of System Manager.</p> | <ul style="list-style-type: none"> <li>• <b>changeIPFQDN - IP &lt;new IP address&gt;</b></li> <li>• <b>changeIPFQDN - FQDN &lt;new fully qualified domain name&gt;</b></li> <li>• <b>changeIPFQDN - IP &lt;new IP address&gt; - GATEWAY &lt;new Gateway address for System Manager&gt; - SEARCH &lt;new search list for DNS address&gt;</b></li> </ul> |

*Table continues...*



| # | Command                   | Parameters                                                                                                                                                                                                                                                                                                                                                              | Description                                                                            | Usage                                                                                                                                                                                                                                                                                                                                                                                        |
|---|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 | <b>changePublicIPFQDN</b> | <ul style="list-style-type: none"> <li>• <b>-publicIP</b> &lt;new IP address for System Manager&gt;</li> <li>• <b>-publicFQDN</b> &lt;new fully qualified domain name for System Manager&gt;</li> <li>• <b>-publicGATEWAY</b> &lt;new Gateway address for System Manager&gt;</li> <li>• <b>-publicNETMASK</b> &lt;new netmask address for System Manager&gt;</li> </ul> | Updates the existing Public IP address, FQDN, Gateway, and Netmask with the new value. | <ul style="list-style-type: none"> <li>• <b>changePublicIPFQDN -publicIP</b> &lt;new Public IP address&gt;</li> <li>• <b>changePublicIPFQDN -publicFQDN</b> &lt;new fully qualified domain name for public interface&gt;</li> <li>• <b>changePublicIPFQDN -publicIP</b> &lt;new Public IP address&gt; <b>-publicGATEWAY</b> &lt;new Public Gateway address for System Manager&gt;</li> </ul> |
| 3 | <b>upgradeSMGR</b>        | <absolute path to the dmutility.bin> -m -v                                                                                                                                                                                                                                                                                                                              | Upgrades System Manager using the data migration utility.                              | <b>upgradeSMGR dmutility *.bin -m -v</b>                                                                                                                                                                                                                                                                                                                                                     |
| 4 | <b>SMGRPachdeploy</b>     | <absolute path to the System Manager service pack or the software patch>                                                                                                                                                                                                                                                                                                | Installs the software patch or the service pack for System Manager.                    | <b>SMGRPachdeploy</b> <absolute path to SMGRservicepackName><br><br> <b>Note:</b><br>Copy the System Manager service pack or patches that you must install to /swlibrary.                                                                                                                               |
| 5 | <b>configureTimezone</b>  | Time zone that you select                                                                                                                                                                                                                                                                                                                                               | Configures the time zone with the value that you select.                               | <b>configureTimeZone</b><br><br>Select a time zone. For example, America/Denver                                                                                                                                                                                                                                                                                                              |

Table continues...

| #  | Command                       | Parameters                 | Description                                                                                                                                                                                                      | Usage                                                                                                                                                                                                                                    |
|----|-------------------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6  | <b>configureNTP</b>           | <IP address of NTP server> | Configures the NTP server details.                                                                                                                                                                               | <b>configureNTP &lt;IP address of NTP server&gt;</b><br><br>Separate IP addresses or hostnames of NTP servers with commas (,).                                                                                                           |
| 7  | <b>createCA</b>               |                            | Creates a new Certificate Authority by using SHA2 signing algorithm and 2048 key size.<br><br>For more information, see, Creating a new Certificate Authority by using SHA2 signing algorithm and 2048 key size. | <b>createCA</b><br><br>You must provide the desired Common Name (CN)                                                                                                                                                                     |
| 8  | <b>configureOOBM</b>          |                            | Enables or disables the Out of Band Management configuration.                                                                                                                                                    | <ul style="list-style-type: none"> <li>To enable Out of Band Management: <b>configureOOBM - EnableOOBM</b></li> <li>To disable Out of Band Management: <b>configureOOBM - DisableOOBM</b></li> </ul>                                     |
| 9  | <b>enableOOBMMultiTenancy</b> |                            | If Out of Band Management and MultiTenancy are enabled on system, use this command to provision tenant administrators to available on public interface.                                                          |                                                                                                                                                                                                                                          |
| 10 | <b>setSecurityProfile</b>     |                            | Enabling the commercial and military grade hardening.                                                                                                                                                            | <ul style="list-style-type: none"> <li>Enabling commercial grade hardening: <b>setSecurityProfile --enable-commercial-grade</b></li> <li>Enabling military grade hardening: <b>setSecurityProfile --enable-military-grade</b></li> </ul> |

Table continues...

| #  | Command                                                                                             | Parameters | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Usage                                                                                                                         |
|----|-----------------------------------------------------------------------------------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 11 | <b>EASGManage</b>                                                                                   |            | Enables or disables EASG.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• <b>EASGManage --enableEASG</b></li> <li>• <b>EASGManage --disableEASG</b></li> </ul> |
| 12 | <b>EASGStatus</b>                                                                                   |            | Displays the status of EASG.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                               |
| 13 | <b>EASGProductCert</b>                                                                              |            | Displays the EASG certificate details.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>EASGProductCert --certInfo</b>                                                                                             |
| 14 | <b>EASGSiteCertManage</b>                                                                           |            | To manage EASG Certificates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                               |
| 15 | <b>editHosts</b>                                                                                    |            | To modify the <code>/etc/hosts</code> file.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                               |
| 16 | <ul style="list-style-type: none"> <li>• <b>swversion</b></li> <li>• <b>swversion -s</b></li> </ul> |            | <ul style="list-style-type: none"> <li>• <b>swversion</b>: Displays the System Manager software information.</li> <li>• <b>swversion -s</b>: Displays the System Manager software version and also displays information about the application name, profile, and deployment type.</li> <li>•  <b>Note:</b><br/>The output varies based on the application deployment and the virtualization environment.</li> </ul> |                                                                                                                               |

*Table continues...*

| #  | Command            | Parameters | Description                                | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----|--------------------|------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17 | <b>changeVFQDN</b> |            | To change the System Manager Virtual FQDN. | <p><b>changeVFQDN</b></p> <p>Type the System Manager Virtual FQDN.</p> <p> <b>Note:</b></p> <p>When you run the <b>changeVFQDN</b> command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.</p> |

*Table continues...*

| #  | Command           | Parameters | Description                                                                                                                  | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-------------------|------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18 | <b>pairIPFQDN</b> |            | Changing the IP address and FQDN on the secondary System Manager server when the secondary is in the standby or active mode. | <ul style="list-style-type: none"> <li>• If you changed both the IP address and FQDN of primary server, type the following on the secondary server:<br/> <pre>#sh \$MGMT_HOME/ utils/ ipfqdnchange/ pairIpFqdnChange.sh -OLDIP &lt;Old IP of the primary server&gt; -NEWIP &lt;New IP of the primary server&gt; - OLDFQDN &lt;Old FQDN of the primary server&gt; -NEWFQDN &lt;New FQDN of the primary server&gt;</pre> </li> <li>• If you changed the IP address of primary server, type the following on secondary server:<br/> <pre>#sh \$MGMT_HOME/ utils/ ipfqdnchange/ pairIpFqdnChange.sh -OLDIP &lt;Old IP of the primary server&gt; -NEWIP &lt;New IP of the primary server&gt;</pre> </li> <li>• If you changed FQDN of primary server, type the following on secondary server:<br/> <pre>#sh \$MGMT_HOME/ utils/ ipfqdnchange/ pairIpFqdnChange.sh -OLDFQDN &lt;Old FQDN of</pre> </li> </ul> |

*Table continues...*

| #  | Command                      | Parameters | Description                                                                                              | Usage                                                                                                                                                                                                                                                                                                                                        |
|----|------------------------------|------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                              |            |                                                                                                          | the primary server> - NEWFQDN <New FQDN of the primary server>                                                                                                                                                                                                                                                                               |
| 19 | <b>smgr</b>                  |            | Starts, stops, and checks the status of Jboss service.                                                   | <b>smgr</b> start/stop/status                                                                                                                                                                                                                                                                                                                |
| 20 | <b>smgr-db</b>               |            | Starts, stops, and checks the status of postgresql.service.                                              | <b>smgr-db</b> start/stop/status                                                                                                                                                                                                                                                                                                             |
| 21 | <b>toggleWebblmOldcert</b>   |            | Replaces identity certificate with old certificate.                                                      | <b>toggleWebblmOldcert</b>                                                                                                                                                                                                                                                                                                                   |
| 22 | <b>getUserAuthCert</b>       |            | Generates a user specific certificate for System Manager to facilitate certificate-based authentication. |                                                                                                                                                                                                                                                                                                                                              |
| 23 | <b>changeCipherSuiteList</b> |            | Configures cipher suite mode for System Manager                                                          | <ul style="list-style-type: none"> <li>To configure strict cipher suite list, type the following command. This would disable CBC ciphers:<br/><b>changeCipherSuiteList LIST2</b></li> <li>To configure relax cipher suite list, type the following command. This would enable CBC ciphers:<br/><b>changeCipherSuiteList LIST1</b></li> </ul> |
| 24 | <b>collectLogs</b>           |            | Collects the required logs.                                                                              | <ul style="list-style-type: none"> <li>To collect all the logs: <b>collectLogs</b></li> <li>To collect all the logs along with backup: <b>collectLogs -Db</b></li> <li>To collect all the logs along with CND data: <b>collectLogs -CND</b></li> </ul>                                                                                       |

Table continues...

| #  | Command                                     | Parameters                     | Description                                                        | Usage                                                                                                                                                                                                                                                                                                                                                                                              |
|----|---------------------------------------------|--------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25 | <b>rebootVM</b>                             |                                | Reboots the System Manager virtual machine.                        | Type <b>y</b> or <b>n</b> to reboot the System Manager virtual machine.                                                                                                                                                                                                                                                                                                                            |
| 26 | <b>powerOffVM</b>                           |                                | Power off the System Manager virtual machine.                      | Type <b>y</b> or <b>n</b> to power off the System Manager virtual machine.                                                                                                                                                                                                                                                                                                                         |
| 27 | sudo /bin/systemctl (parameter) snmpd       | start/stop/restart/status      | To start or stop, and to check status of the SNMP service.         |                                                                                                                                                                                                                                                                                                                                                                                                    |
| 28 | sudo /bin/systemctl (parameter) spiritAgent | start/stop/restart/status      | To start or stop, and to check status of the Spirit Agent service. |                                                                                                                                                                                                                                                                                                                                                                                                    |
| 29 | sudo /bin/systemctl (parameter) cnd         | start/stop/restart/status      | To start or stop, and to check status of the CND service.          |                                                                                                                                                                                                                                                                                                                                                                                                    |
| 30 | encryptionPassphrase                        | [add   change   remove   list] | To add, change, remove, and display the encryption passphrase.     | <ul style="list-style-type: none"> <li>• <b>encryptionPassphrase add:</b> To add encryption passphrase.</li> <li>• <b>encryptionPassphrase change:</b> To change existing encryption passphrase.</li> <li>• <b>encryptionPassphrase remove:</b> To remove encryption passphrase.</li> <li>• <b>encryptionPassphrase list:</b> To display the encryption passphrase and slot assignment.</li> </ul> |

*Table continues...*

| #  | Command                            | Parameters                                | Description                                          | Usage                                                                                                                                                                                                                                                                                      |
|----|------------------------------------|-------------------------------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31 | <code>encryptionRemoteKey</code>   | [add   remove   list]                     | To add, remove, and display the remote key server.   | <ul style="list-style-type: none"> <li>• <b>encryptionRemoteKey add:</b> To add remote key server.</li> <li>• <b>encryptionRemoteKey remove:</b> To remove remote key server.</li> <li>• <b>encryptionRemoteKey list:</b> To display the remote key server and slot assignment.</li> </ul> |
| 32 | <code>encryptionLocalKey</code>    | [enable   disable]                        | To enable and disable the local key store.           | <ul style="list-style-type: none"> <li>• <b>encryptionLocalKey enable:</b> To enable local key store.</li> <li>• <b>encryptionLocalKey disable:</b> To disable local key store.</li> </ul>                                                                                                 |
| 33 | <code>encryptionStatus</code>      |                                           | Displays information about encryption on the system. | <b>encryptionStatus</b> displays information about encryption on the system.                                                                                                                                                                                                               |
| 34 | <code>updateLogRetention.sh</code> | [-p] [-v]<br>[maxRetentionTime]           | Manages the log retention time.                      |                                                                                                                                                                                                                                                                                            |
| 35 | <code>pruneAllLogs.sh</code>       | [-b] [-t] [-v] [-h]<br>[maxRetentionTime] | Manages the deletion of log files.                   |                                                                                                                                                                                                                                                                                            |

*Table continues...*



| #  | Command                           | Parameters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Description                                                                                                                                                                                                                           | Usage |
|----|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 36 | <b>manageEntityClassWhitelist</b> | [-h] [addAll -e<br><ENTITY_CLASS_NAME><br>-f <INPUT_FILE> -u<br><USERNAME> -p<br><PASSWORD>] [add -e<br><ENTITY_CLASS_NAME><br>-s <SUBJECT_NAME> -u<br><USERNAME> -p<br><PASSWORD>] [list -e<br><ENTITY_CLASS_NAME><br>-f <OUTPUT_FILE> -u<br><USERNAME> -p<br><PASSWORD> -pn<br><PAGENUMBER> -ps<br><PAGESIZE>] [view -e<br><ENTITY_CLASS_NAME><br>-s <SUBJECT_NAME> -f<br><OUTPUT_FILE> -u<br><USERNAME> -p<br><PASSWORD>]<br>[subjectCheck -e<br><ENTITY_CLASS_NAME><br>-u <USERNAME> -p<br><PASSWORD>] [deleteAll<br>-e<br><ENTITY_CLASS_NAME><br>-u <USERNAME> -p<br><PASSWORD>] [delete -e<br><ENTITY_CLASS_NAME><br>-s <SUBJECT_NAME> -u<br><USERNAME> -p<br><PASSWORD>] | <p>You can add, list, view, and delete the subject names for the provided entity class.</p> <p>You can add and delete the bulk entries of subject names and check the status of the subject name validation for the entity class.</p> |       |
| 37 | <b>outboundConnectionLogging</b>  | [enable] [disable]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | If you enable this, you can capture the logs in the <code>/var/log/Avaya/connections</code> file for every new outgoing connections initiated from System Manager.                                                                    |       |
| 38 | <b>configureOutboundFirewall</b>  | [add {-s} {-f}] [list] [status]<br>[remove {-e} {-f}] [disable]<br>[overwrite {-s} {-f}] [enable-logging]<br>[disable-logging]<br>[logging-status]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | If you enable this, you can configure System Manager outbound firewall.                                                                                                                                                               |       |

*Table continues...*

| #  | Command                  | Parameters                                                          | Description                                                                                                                                                                                                                                                             | Usage |
|----|--------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 39 | <b>setSecurityPolicy</b> | [--status] [--display-only] [--restore-standard] [--refresh-custom] | You can modify the default password policy settings of System Manager by using the <b>setSecurityPolicy</b> command. This command is only applicable for changing or setting up the password for the CLI user or root user that gets created at the time of deployment. |       |

# Chapter 27: Configuring the date and time

---

## Verifying changes to the date and time configuration

### Procedure

1. Log in to System Manager from the command line.
2. Type the date, and press `Enter`.  
The system displays the updated date, time, and time zone values. Verify the values.
3. Type `exit` and press `Enter`.

---

## Configuring System Manager logs for Syslog server

### About this task

Use this procedure to:

- Direct System Manager security logs to remote Syslog server.
- Configure general and security logs for the Syslog server.
- Configure security audit logs for the Syslog server.

### Procedure

1. On the System Manager web console, click **Services > Events > Logs > Log Settings**.
2. On the Log Settings page, in the **Logger** column, click `com.avaya.security.iam.audit`.
3. Click **Edit**.
4. On the Edit Logger page, click **Attach**.
5. On the Attach Appender page, in the **Select Appender** field, click **SYSLOG**.
6. Click **Commit**.  
System Manager adds SYSLOG as an appender for the audit log.
7. **(Optional)** To modify the Syslog configuration, select the SYSLOG appender, and click **Edit**.

---

## Changing date and time on System Manager running on VMware

---

### Configuring the NTP server

#### Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.

#### Procedure

Type `configureNTP <IP address of NTP server>`.

#### Related links

[System Manager command line interface operations](#) on page 1518

---

### Configuring the time zone

#### About this task

When you run the `configureTimeZone` command, it restarts the database connection.

#### Before you begin

- To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the **Console** tab or the  icon.
  - Use PuTTY.
- Log in to System Manager with administrator privilege credentials.

#### Procedure

1. Type `configureTimeZone` on the System Manager command line interface.
2. Select the time zone from the list.  
For example, America/Denver.
3. Reboot the system to reflect the time zone changes.

#### Related links

[System Manager command line interface operations](#) on page 1518

# Chapter 28: System Manager localization

When you install the language pack on System Manager, the following user interface screens support the Canadian French localization:

- Authentication page.

Localization changes are not available for System Manager Dashboard.

- On User Management, in **Communication Profile**, localized pages are available for **Session Manager**, **Communication Manager**, and **Messaging** profiles.

 **Note:**

Localized pages are not available for following:

- Password change/management pages
- In **Communication Profile**, profiles for Collaboration Environment, CS1000, Callpilot, IP Office, Presence, Conferencing, and Work Assignment.
- Membership and Contact pages
- Communication Manager management
  - Edit Endpoint Extension on the Manage Endpoints page.
  - On the Maintenance page, **Release Endpoint**, **Busyout Endpoint**, **Test Endpoint**, **List Trace Station** and **Status Station** pages In “”
  - On the Edit Endpoint page, **General Options**, **Group Membership**, **Feature Options**, **Site Data**, **Abbreviated Call Dialing**, **Enhanced Call Fwd**, **Button Assignment** and **Profile Settings**.
- Messaging Management

On **Messaging > Subscriber > Edit Subscriber**, **Basic Information**, **Subscriber Directory**, **Subscriber Security**, **Mailbox Features**, **Secondary Extensions** and **Miscellaneous**.

## Related links

[Installing language pack on System Manager](#) on page 1532

---

## Installing language pack on System Manager

### About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

 **Note:**

After installing the language pack, you cannot uninstall the language pack.

### Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.
2. Type `locate LocalizationScript.sh`, and press Enter.

System Manager displays the path of the localization script.

For example: `/opt/Avaya/Mgmt/8.1.x/CommonConsole/script/LocalizationScript.sh`

3. Type `locate FrenchResourceBundle.zip`, and press Enter.

The System Manager displays the path of the `FrenchResourceBundle.zip` script.

For example: `/opt/Avaya/Mgmt/8.1.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

This is just an example of the path; the path might vary based on actual path that you get.

4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.
5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/CommonConsole/localization/common_console/FrenchResourceBundle.zip`.
6. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection.

If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

 **Note:**

During this activity, System Manager restarts the JBoss service. Therefore, the System Manager web console will not be accessible. If System Manager is in the Geographic Redundancy mode, then apply these steps on the secondary System Manager server also after secondary server is active.

7. Change the browser language setting to French.

### Related links

[System Manager localization](#) on page 1531

# Chapter 29: Resources

## System Manager documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at <http://support.avaya.com>.

| Title                                                                  | Description                                                                                   | Audience                                             |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------|
| Design                                                                 |                                                                                               |                                                      |
| <i>Avaya Aura® System Manager Overview and Specification</i>           | Understand high-level product features and functionality.                                     | Customers and sales, services, and support personnel |
| <i>Administering Avaya Aura® System Manager</i>                        | Administering System Manager applications and install patches on System Manager applications. | Customers and sales, services, and support personnel |
| <i>Avaya Aura® System Manager Certificate Management</i>               | Understand certificate management.                                                            | Customers and sales, services, and support personnel |
| <i>Avaya Aura® System Manager Data Privacy Guidelines</i>              | Describes how to administer System Manager to fulfill Data Privacy requirements.              | System administrators and IT personnel               |
| Using                                                                  |                                                                                               |                                                      |
| <i>Using the Solution Deployment Manager client</i>                    | Deploy System Manager applications and install patches on System Manager applications.        | System administrators                                |
| <i>Avaya Aura® System Manager Solution Deployment Manager Job-Aid</i>  | Deploy System Manager applications and install patches on System Manager applications.        | System administrators                                |
| Implementation                                                         |                                                                                               |                                                      |
| <i>Upgrading Avaya Aura® System Manager</i>                            | Upgrade the Avaya Aura® System Manager application to Release 8.1.x.                          | Implementation personnel                             |
| <i>Deploying Avaya Aura® System Manager in Virtual Appliance</i>       | Deploy System Manager applications in Virtual Appliance.                                      | Implementation personnel                             |
| <i>Deploying Avaya Aura® System Manager in Virtualized Environment</i> | Deploy System Manager applications in Virtualized Environment.                                | Implementation personnel                             |

Table continues...

| Title                                                                                  | Description                                                                                                                 | Audience                               |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| <i>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</i> | Deploy System Manager applications in Infrastructure as a Service Environment.                                              | Implementation personnel               |
| <i>Deploying Avaya Aura® System Manager in Software-Only Environment</i>               | Deploy System Manager applications in Software-Only Environment.                                                            | Implementation personnel               |
| Maintenance and Troubleshooting                                                        |                                                                                                                             |                                        |
| <i>Avaya Aura® System Manager Fault Management and monitoring using SNMP</i>           | Monitor System Manager using SNMP.                                                                                          | System administrators and IT personnel |
| <i>Troubleshooting Avaya Aura® System Manager</i>                                      | Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports. | System administrators and IT personnel |

---

## Finding documents on the Avaya Support website

### Procedure

1. Go to <https://support.avaya.com>.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.  
The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.  
For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

---

## Accessing the port matrix document

### Procedure

1. Go to <https://support.avaya.com>.
2. Log on to the Avaya website with a valid Avaya user ID and password.



3. On the Avaya Support page, click **Support by Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or both the following categories:
  - **Application & Technical Notes**
  - **Design, Development & System Mgt**

The list displays the product-specific Port Matrix document.
7. Click **Enter**.

---

## Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at <https://documentation.avaya.com>.

### Important:

For documents that are not available on Avaya Documentation Center, click **More Sites > Support** on the top menu to open <https://support.avaya.com>.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** (  ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (  ).

Navigate to the **Manage Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon (  ).

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

 **Note:**

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

---

## Training

The following courses are available on the Avaya Learning website at <http://www.avaya-learning.com>. After you login to the website, enter the course code or the title in the **Search** field and click **Go** to search for the course.

| Course code | Course title                                                               |
|-------------|----------------------------------------------------------------------------|
| 20460W      | Virtualization and Installation Basics for Avaya Team Engagement Solutions |
| 20970W      | Introducing Avaya Device Adapter                                           |
| 20980W      | What's New with Avaya Aura® Release 8.1                                    |
| 71200V      | Integrating Avaya Aura® Core Components                                    |
| 72200V      | Supporting Avaya Aura® Core Components                                     |
| 20130V      | Administering Avaya Aura® System Manager Release 8.1                       |
| 21450V      | Administering Avaya Aura® Communication Manager Release 8.1                |

---

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

## About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://www.youtube.com/AvayaMentor) and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

 **Note:**

Videos are not available for all products.

---

## Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

### Related links

[Using the Avaya InSite Knowledge Base](#) on page 1537

---

## Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation

- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <http://www.avaya.com/support>.
2. Log on to the Avaya website with a valid Avaya user ID and password.  
The system displays the Avaya Support page.
3. Click **Support by Product > Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press **Enter**.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

### Related links

[Support](#) on page 1537

# Appendix A: Firewall implementation in System Manager

---

## Firewall basics

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources. The firewall controls what outside resources its own users can have access to. Simply put, a firewall is a program or a hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters it is not allowed through.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

- Packet filtering - Packets or small chunks of data are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- Stateful inspection - A newer method that does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match the information is allowed through. Else, it is discarded.

---

## Firewall implementation in System Manager

The System Manager firewall implementation uses packet filtering and stateful inspection techniques. The System Manager firewall provides the following:

- Supports unlimited access to loop back address through packet filtering.
- Drops all inbound packets by default, allows all outbound packets, and allows all packets that are to be forwarded through packet filtering.

- For TCP packets, the firewall checks for various combinations of the TCP flags to ascertain whether a packet is valid or not. The System Manager firewall implementation includes a set of standard rules for identifying valid TCP packets.
- Supports stateful inspection of packets. The firewall checks the state of all inbound and outbound packets for secure communication. For inbound packets the state must be either Established or Related. For outbound packets the state must be either New, Established or Related.
- Disables ICMP timestamp responses as this allows an attacker to know the date which is set on your machine. This defeats all the time based authentication protocols.
- Allows inbound communication on ports that are exposed for interactions with various Avaya Aura® products.

# Appendix B: Communication Manager reports available through System Manager

---

## List reports

System Manager supports the following list reports.

- aar analysis
- aar digit-conversion
- aar route-chosen
- abbreviated-dialing group
- abbreviated-dialing personal
- aca-parameters
- access-endpoint
- administered-connection
- agent-loginid
- announcements
- ars analysis
- ars digit-conversion
- ars route-chosen
- asq-history
- attendant
- audio-group
- authorization-code
- bcms agent
- bcms skill
- bcms split
- bcms summary agent
- bcms summary skill

- bcms summary split
- bcms summary trunk
- bcms summary vdn
- bcms trunk
- bcms vdn
- bcms-vustats loginIDs
- best-service-routing
- bridged-extensions
- cabinet
- call-forwarding
- calltype
- configuration all
- configuration board
- configuration carrier
- configuration control
- configuration ds1
- configuration firmware-versions
- configuration media-gateway
- configuration port-network
- configuration power-supply
- configuration radio-controller
- configuration software-versions
- configuration stations
- configuration trunks
- configuration wt-stations
- cor
- coverage answer-group
- coverage path
- coverage time-of-day
- crm-features
- cti-link
- data-module
- directory board
- disabled-mos



- do-not-disturb group
- do-not-disturb station
- eda-external-device-alm
- emergency
- extended-pickup-group
- extension-type
- group-page
- groups-of-extension
- history
- holiday-table
- hunt-group
- internal-data loginID
- integrated-annc-boards
- intercom-group
- intra-switch-cdr
- ip-codec-set
- ip-interface
- ip-network-map
- ip-network-region direct-wan
- ip-network-region igar-dpt
- ip-network-region monitor
- ip-network-region qos
- ip-route
- ipserver-interface
- isdnpri-testcall
- logins
- marked-ports
- mct-history
- measurements aca
- measurements announcements board last-hour
- measurements announcements board today-peak
- measurements announcements board yesterday-peak
- measurements announcements all last-hour
- measurements announcements all today-peak

- measurements announcements all yesterday-peak
- measurements attendant group
- measurements attendant positions
- measurements blockage pn last-hour
- measurements blockage pn today-peak
- measurements blockage pn yesterday-peak
- measurements call-rate data
- measurements call-rate multimedia
- measurements call-rate service-link
- measurements call-rate total
- measurements call-rate voice
- measurements call-summary
- measurements cbc-trunk-group last-hour
- measurements cell-traffic cell-addr last-hour
- measurements cell-traffic cell-addr today-peak
- measurements cell-traffic cell-addr yesterday-peak
- measurements cell-traffic summary last-hour
- measurements cell-traffic summary today-peak
- measurements cell-traffic summary yesterday-peak
- measurements clan ethernet
- measurements clan sockets detail last-hour
- measurements clan sockets detail today-peak
- measurements clan sockets detail yesterday-peak
- measurements clan sockets hourly
- measurements clan sockets summary last-hour
- measurements clan sockets summary today-peak
- measurements clan sockets summary yesterday-peak
- measurements communications-links 1-8
- measurements communications-links 9-16
- measurements communications-links 17-24
- measurements communications-links 25-32
- measurements communications-links 33
- measurements coverage-path last-hour
- measurements coverage-path today-peak

- measurements coverage-path yesterday-peak
- measurements ds1 log
- measurements ds1 summary
- measurements ds1-facility log
- measurements ds1-facility summary
- measurements expansion-services-mod hourly
- measurements expansion-services-mod summary last-hour
- measurements expansion-services-mod summary today-peak
- measurements expansion-services-mod summary yesterday-peak
- measurements hunt-group last-hour
- measurements hunt-group today-peak
- measurements hunt-group yesterday-peak
- measurements ip codec detail last-hour
- measurements ip codec detail today-peak
- measurements ip codec detail yesterday-peak
- measurements ip codec hourly
- measurements ip codec summary last-hour
- measurements ip codec summary today-peak
- measurements ip codec summary yesterday-peak
- measurements ip dsp-resource detail last-hour
- measurements ip dsp-resource detail today-peak
- measurements ip dsp-resource detail yesterday-peak
- measurements ip dsp-resource hourly
- measurements ip dsp-resource summary last-hour
- measurements ip dsp-resource summary today-peak
- measurements ip dsp-resource summary yesterday-peak
- measurements ip signaling-groups current-hour
- measurements ip signaling-groups last-hour
- measurements ip signaling-groups today
- measurements ip signaling-groups yesterday
- measurements lar-route-pattern last-hour
- measurements lar-route-pattern today
- measurements lar-route-pattern yesterday
- measurements lightly-used-trunk last-hour

- measurements lightly-used-trunk today
- measurements lightly-used-trunk yesterday
- measurements load-balance incoming last-hour
- measurements load-balance incoming today-peak
- measurements load-balance incoming yesterday-peak
- measurements load-balance intercom last-hour
- measurements load-balance intercom today-peak
- measurements load-balance intercom yesterday-peak
- measurements load-balance outgoing last-hour
- measurements load-balance outgoing today-peak
- measurements load-balance outgoing yesterday-peak
- measurements load-balance tandem last-hour
- measurements load-balance tandem today-peak
- measurements load-balance tandem yesterday-peak
- measurements load-balance total last-hour
- measurements load-balance total today-peak
- measurements load-balance total yesterday-peak
- measurements modem-pool last-hour
- measurements modem-pool today-peak
- measurements modem-pool yesterday-peak
- measurements multimedia-interface hourly
- measurements multimedia-interface last-hour
- measurements multimedia-interface today-peak
- measurements multimedia-interface yesterday-peak
- measurements occupancy busiest-intervals
- measurements occupancy last-hour
- measurements occupancy summary
- measurements outage-trunk last-hour
- measurements outage-trunk today
- measurements outage-trunk yesterday
- measurements principal last-hour
- measurements principal today-peak
- measurements principal yesterday-peak
- measurements route-pattern last-hour

- measurements route-pattern today
- measurements route-pattern yesterday
- measurements security-violations detail
- measurements security-violations summary
- measurements summary
- measurements tone-receiver detail last-hour
- measurements tone-receiver detail today-peak
- measurements tone-receiver detail yesterday-peak
- measurements tone-receiver summary last-hour
- measurements tone-receiver summary today-peak
- measurements tone-receiver summary yesterday-peak
- measurements trunk-group hourly
- measurements trunk-group summary last-hour
- measurements trunk-group summary today-peak
- measurements trunk-group summary yesterday-peak
- measurements voice-conditioners hourly
- measurements voice-conditioners summary last-hour
- measurements voice-conditioners summary today-peak
- measurements voice-conditioners summary yesterday-peak
- measurements wideband-trunk-group hourly
- measurements wideband-trunk-group summary last-hour
- measurements wideband-trunk-group summary today-peak
- measurements wideband-trunk-group summary yesterday-peak
- media-gateway
- meet-me-vdn
- members hunt-group
- members trunk-group
- mmi
- modem-pool
- moh-analog-group
- monitored-station
- mst
- multimedia endpoints
- multimedia h.320-stations

- multimedia ip-stations
- multimedia ip-unregistered
- node-routing
- node-names
- off-pbx-telephone station-mapping
- partition-route-table
- partitioned-group
- performance attendant today
- performance attendant yesterday
- performance hunt-group today
- performance hunt-group yesterday
- performance summary today
- performance summary yesterday
- performance trunk-group today
- performance trunk-group yesterday
- personal-co-line
- pickup-group
- pms-down
- policy-routing-table
- precedence-routing analysis
- precedence-routing digit-conversion
- precedence-routing route-chosen
- pri-endpoint
- private-numbering
- public-unknown-numbering
- registered-ip-stations
- remote-office
- report-scheduler
- route-pattern
- service-hours-table
- set-data
- signaling-group
- sip-station
- skill-status

- station
- stn-firmware
- survivable-processor
- suspend-alm-orig
- synchronization
- sys-link
- term-ext-group
- toll all
- toll restricted-call
- toll toll-list
- toll unrestricted-call
- trace
- trunk-group
- tti-ip-stations
- uniform-dialplan
- usage button-type crss-alert
- usage button-type hunt-ns
- usage button-type night-serv
- usage button-type trunk-ns
- usage cti-link
- usage digit-string
- usage extension
- usage holiday-table
- usage hunt-group
- usage ip-address
- usage node-name
- usage variables
- usage vector
- user-profiles
- vdn
- vector
- video-bridge
- vrt
- vustats-display-format

- wakeup incomplete
- wakeup requests
- wakeup station
- xmobile mapping

System Manager does not support the CSV report format for the following list reports.

- configuration radio-controller
- configuration software-versions
- configuration wt-stations
- measurements call-rate data
- measurements call-rate multimedia
- measurements call-rate service-link
- measurements call-rate total
- measurements call-rate voice
- measurements call-summary
- measurements cell-traffic cell-addr last-hour
- measurements cell-traffic cell-addr today-peak
- measurements cell-traffic cell-addr yesterday-peak
- measurements cell-traffic summary last-hour
- measurements cell-traffic summary today-peak
- measurements cell-traffic summary yesterday-peak
- measurements summary
- measurements tone-receiver summary last-hour
- measurements tone-receiver summary today-peak
- measurements tone-receiver summary yesterday-peak
- mmi
- mct-history
- measurements ds1-facility log
- measurements ds1-facility summary
- measurements principal last-hour
- measurements principal today-peak
- measurements principal yesterday-peak



---

# Display reports

System Manager supports the following display reports.

 **Note:**

System Manager does not support the CSV report format for display reports.

- aar analysis
- aar digit-conversion
- abbreviated-dialing 7103A-buttons
- abbreviated-dialing enhanced
- abbreviated-dialing group
- abbreviated-dialing personal
- abbreviated-dialing system
- access-endpoint
- adjunct-names
- administered-connection
- agent-loginid
- alarms
- alias station
- alphanumeric-dial-table
- alternate-fri
- announcement
- ars analysis
- ars digit-conversion
- ars toll
- attendant
- audio-group
- authorization-code
- bcms-vustats loginIDs
- best-service-routing
- bp
- bri-trunk-board
- bulletin-board
- button-labels
- button-location-aca

- cabinet
- call-screening
- call-type
- cama-numbering
- capacity
- carrier-frequencies
- circuit-packs
- communication-interface links
- communication-interface processor-channels
- console-parameters
- cor
- cos
- cos-group
- coverage answer-group
- coverage path
- coverage remote
- coverage sender-group
- coverage time-of-day
- cti-link
- data-module
- daylight-savings-rules
- dialplan analysis
- dialplan parameters
- digit-absorption
- display-messages ad-programming
- display-messages auto-wakeup-dn-dst
- display-messages button-labels
- display-messages call-identifiers
- display-messages date-time
- display-messages leave-word-calling
- display-messages malicious-call-trace
- display-messages miscellaneous-features
- display-messages posted-message
- display-messages property-management

- display-messages self-administration
- display-messages softkey-labels
- display-messages time-of-day-routing
- display-messages transfer-conference
- display-messages view-buttons
- display-messages vustats
- ds1
- eda-external-device-alm
- enp-number-plan
- errors
- ethernet-options
- events
- extended-pickup-group
- failed-ip-network-region
- feature-access-codes
- firmware download
- firmware station-download
- group-page
- holiday-table
- hunt-group
- inc-call-handling-trmt
- initcauses
- integrated-ann-c-boards
- intercom-group
- intra-switch-cdr
- ip-codec-set
- ip-interface
- ip-network-map
- ip-network-region
- ip-parameters
- ip-route
- ip-services
- ipserver-interface
- isdn dcs-qsig-tsc-gateway

- isdn mwi-prefixes
- isdn network-facilities
- isdn private-numbering
- isdn public-unknown-numbering
- isdn qsig-dcs-tsc-gateway
- isdn tsc-gateway
- ixc-codes
- listed-directory-numbers
- location-parameters
- locations
- login
- lsp
- mct-group-extensions
- meas-selection coverage
- meas-selection principal
- meas-selection route-pattern
- meas-selection trunk-group
- meas-selection wideband-trunk-group
- media-gateway
- modem-pool
- mst
- multifrequency-signaling
- node-names audix
- node-names ip
- node-routing
- off-pbx-telephone configuration-set
- off-pbx-telephone feature-name-extensions
- off-pbx-telephone station-mapping
- paging code-calling-ids
- paging loudspeaker
- partition-route-table
- permissions
- personal-CO-line
- pickup-group

- port
- precedence-routing analysis
- precedence-routing digit-conversion
- pri-endpoint
- private-numbering
- public-unknown-numbering
- radio-controller
- reason-code-names
- remote-access
- remote-office
- rhnpa
- route-pattern
- service-hours-table
- signaling-group
- sit-treatment
- site-data
- software
- station
- svn-button-location
- synchronization
- system-parameters cdr
- system-parameters country-options
- system-parameters coverage-forwarding
- system-parameters crisis-alert
- system-parameters customer-options
- system-parameters duplication
- system-parameters features
- system-parameters hospitality
- system-parameters ip-options
- system-parameters ipserver-interface
- system-parameters maintenance
- system-parameters mlpp
- system-parameters multifrequency-signaling
- system-parameters ocm-call-classification

- system-parameters offer-options
- system-parameters security
- system-parameters special-applications
- system-parameters wireless
- telecommuting-access
- tenant
- term-ext-group
- terminal-parameters
- tftp-server
- time
- time-of-day
- toll
- tone-generation
- trunk-group
- uniform-dialplan
- variables
- vdn
- vector
- video-bridge
- vrt
- vustats-display-format
- xmobile configuration-set

---

## Status reports

System Manager supports the following status reports.

- access-endpoint
- administered-connection
- aesvcs cti-link
- aesvcs interface
- aesvcs link
- attendant
- audits cumulative

- audits peak-hour
- bri-port
- cabinet
- cdr-link
- clan-al
- clan-port
- data-module
- environment
- esm
- ess clusters
- ess port-networks
- firmware station-download
- firmware download
- hardware-group
- health
- ip-board
- ip-network-region
- ip-synchronization master
- ip-synchronization oos-members
- ip-synchronization system-information
- ip-synchronization member media-gateway
- ip-synchronization source media-gateway
- isdnpri-testcall
- journal-link
- link
- logins
- media-gateways
- media-processor all
- media-processor board
- mg-announcements
- meet-me-vdn
- mst
- nr-registration all-regions
- nr-registration network-region

- nr-registration survivable-processor
- off-pbx-telephone mapping-subscriptions
- off-pbx-telephone station
- packet-interface
- periodic-scheduled
- pms-link
- pnc
- port-network
- pri-endpoint
- processor-channels
- psa
- qos-parameters ipserver-interface
- remote-access
- remote-office
- signaling-group
- sp-link
- socket-usage
- station
- switch-node
- synchronization
- sys-link
- trace-analyzer
- trunk
- tsc-administered
- tti
- val-ip
- video-bridge

System Manager supports the CSV report format for the following status reports.

- aesvcs cti-link
- aesvcs interface
- aesvcs link
- clan-al
- ess clusters
- ess port-networks



- ip-synchronization master
- ip-synchronization oos-members
- ip-synchronization member media-gateway
- ip-synchronization source media-gateway
- isdnpri-testcall
- media-processor all
- mg-announcements
- off-pbx-telephone mapping-subscriptions
- qos-parameters ipserver-interface
- switch-node
- synchronization
- trunk
- tsc-administered

# Appendix C: Remote Access

---

## Remote access of System Manager

To provide remote and online support, Avaya services personnel can remotely access the System Manager application by using Enhanced Access Security Gateway (EASG)

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

The product must be registered using the Avaya Global Registration Tool for enabling the system for Avaya Remote Connectivity.

You can also enable EASG after deploying or upgrading the application by using the command:  
**EASGManage --enableEASG.**

For more information about EASG, see *Deploying Avaya Aura® System Manager in Virtual Appliance*.

---

## EASG login for System Manager

From System Manager Release 7.1.2 and later, Avaya Technician can use the EASG user accounts to access the System Manager web console and Command Line Interface. Following are the EASG user accounts:

- **init:** Provides the System Administrator role.
- **craft:** Provides the Avaya Services and Maintenance support.

The init and craft accounts are built-in user accounts. Therefore, you cannot modify these user accounts. If EASG is disabled, the system removes the user accounts from System Manager.

---

# Logging on to the System Manager web console by using EASG login

## About this task

Avaya Technician and Avaya Services can use the following procedure to login to the System Manager web console by using EASG login.

## Before you begin

EASG must be enabled.

## Procedure

1. On the web browser, do one of the following:

- If you are in a customer network, type `https://<System Manager_Fully Qualified Domain Name>/services`.
- If you are not in the customer network and using the Secure Access Link (SAL) https connection, type `https://localhost/services` or `https://127.0.0.1/services`.

If you are neither in the customer network nor using the Secure Access Link (SAL) https connection then you cannot access the System Manager web console.

If EASG is disabled, the system displays the message: `EASG is disabled`.

If EASG is enabled, proceed with the following steps.

2. In the **Username** field, type `init` or `craft`.
3. Click **Next**.

The system displays the **Challenge**, **Product ID**, and **Response** fields. The **Challenge** and **Product ID** fields are read only.

4. In **Response**, paste the response for the EASG challenge.

The response is up to 512 characters long.

5. Click **Login**.

The system validates the challenge and response. If authentication is successful, the system displays the System Manager web console.

# Index

## Special Characters

|                                             |                                           |
|---------------------------------------------|-------------------------------------------|
| _field descriptions                         |                                           |
| Adding AES instance to System Manager ..... | <a href="#">951</a>                       |
| .CADF xml file to MIB and trapd file .....  | <a href="#">955</a> , <a href="#">956</a> |

## Numerics

|                     |                      |
|---------------------|----------------------|
| 2048 key size ..... | <a href="#">1216</a> |
| 7.0 .....           | <a href="#">1404</a> |

## A

|                                                            |                                           |
|------------------------------------------------------------|-------------------------------------------|
| AAR/ARS Digit Conversion field descriptions                |                                           |
| AAR/ARS Digit Conversion; field description .....          | <a href="#">797</a> , <a href="#">799</a> |
| Abbreviated Dialing                                        |                                           |
| Enhanced List .....                                        | <a href="#">755</a>                       |
| Abbreviated Dialing List 1, List 2, List 3 .....           | <a href="#">755</a>                       |
| abbreviated dialing lists .....                            | <a href="#">755</a>                       |
| abort                                                      |                                           |
| global user settings import job on first error .....       | <a href="#">406</a>                       |
| abort a user import job .....                              | <a href="#">398</a>                       |
| abort global user settings import job on first error ..... | <a href="#">406</a>                       |
| aborting                                                   |                                           |
| virtual machine report generation .....                    | <a href="#">1376</a>                      |
| about audio files .....                                    | <a href="#">1147</a>                      |
| about CM audit .....                                       | <a href="#">979</a>                       |
| about reports .....                                        | <a href="#">1082</a>                      |
| Access Control .....                                       | <a href="#">181</a>                       |
| Accessing Element Cut-Through .....                        | <a href="#">709</a>                       |
| accessing log harvest .....                                | <a href="#">1004</a>                      |
| accessing port matrix .....                                | <a href="#">1534</a>                      |
| accessing resources .....                                  | <a href="#">175</a>                       |
| accessing scheduler .....                                  | <a href="#">1097</a>                      |
| accessing the Backup and Restore service .....             | <a href="#">841</a>                       |
| accessing the Data Retention Rules service                 |                                           |
| data retention rules service; access .....                 | <a href="#">861</a>                       |
| accessing the Log Settings service .....                   | <a href="#">1017</a>                      |
| accessing WebLM .....                                      | <a href="#">1032</a>                      |
| access log harvesting .....                                | <a href="#">1004</a>                      |
| access profile .....                                       | <a href="#">936</a>                       |
| create .....                                               | <a href="#">920</a>                       |
| delete .....                                               | <a href="#">921</a>                       |
| modify .....                                               | <a href="#">921</a>                       |
| new .....                                                  | <a href="#">920</a>                       |
| remove .....                                               | <a href="#">921</a>                       |
| access Solution Deployment Manager client .....            | <a href="#">1283</a>                      |
| Access to Administrative Users .....                       | <a href="#">220</a>                       |
| access to PLDS .....                                       | <a href="#">1287</a>                      |
| account operations                                         |                                           |
| CS1000 .....                                               | <a href="#">985</a>                       |
| account synchronization .....                              | <a href="#">980</a>                       |
| activate SSH from AVP Utilities .....                      | <a href="#">1332</a>                      |

|                                                  |                                                                 |
|--------------------------------------------------|-----------------------------------------------------------------|
| activating                                       |                                                                 |
| secondary server .....                           | <a href="#">113</a>                                             |
| activating agent .....                           | <a href="#">968</a>                                             |
| activating serviceability agent .....            | <a href="#">968</a>                                             |
| Active                                           |                                                                 |
| Coverage Path .....                              | <a href="#">703</a>                                             |
| Active Station Ringing .....                     | <a href="#">740</a>                                             |
| Act Time .....                                   | <a href="#">708</a>                                             |
| actual license usage .....                       | <a href="#">1034</a>                                            |
| add                                              |                                                                 |
| custom role .....                                | <a href="#">187</a>                                             |
| custom tenant administrator role .....           | <a href="#">189</a>                                             |
| endpoints .....                                  | <a href="#">712</a>                                             |
| G430 Branch Gateway .....                        | <a href="#">928</a>                                             |
| G450 Branch Gateway .....                        | <a href="#">928</a>                                             |
| hunt group .....                                 | <a href="#">780</a>                                             |
| new role .....                                   | <a href="#">187</a>                                             |
| new tenant administrator role .....              | <a href="#">189</a>                                             |
| role .....                                       | <a href="#">187</a>                                             |
| add a contact address of a private contact ..... | <a href="#">284</a>                                             |
| add a contact address of a public contact .....  | <a href="#">596</a>                                             |
| Add Address page .....                           | <a href="#">256</a> , <a href="#">290</a> , <a href="#">606</a> |
| add a postal address to public contact .....     | <a href="#">595</a>                                             |
| add a public contact .....                       | <a href="#">593</a>                                             |
| add element access profile .....                 | <a href="#">909</a>                                             |
| add element instances .....                      | <a href="#">1043</a>                                            |
| Add elements                                     |                                                                 |
| bulk .....                                       | <a href="#">898</a>                                             |
| manual .....                                     | <a href="#">898</a>                                             |
| Add elements in bulk .....                       | <a href="#">898</a>                                             |
| Add End Entity .....                             | <a href="#">1213</a>                                            |
| add endpoints                                    |                                                                 |
| field descriptions .....                         | <a href="#">735</a>                                             |
| add endpoints in bulk .....                      | <a href="#">769</a>                                             |
| add endpoint templates                           |                                                                 |
| field descriptions .....                         | <a href="#">735</a>                                             |
| Add Entity Class                                 |                                                                 |
| field descriptions .....                         | <a href="#">1203</a>                                            |
| adding                                           |                                                                 |
| Appliance Virtualization Platform host .....     | <a href="#">1319</a>                                            |
| AVP host .....                                   | <a href="#">1319</a>                                            |
| Communication Manager .....                      | <a href="#">926</a>                                             |
| communication profile for user .....             | <a href="#">258</a>                                             |
| encryption passphrase .....                      | <a href="#">1491</a>                                            |
| ESXi host .....                                  | <a href="#">1319</a>                                            |
| location .....                                   | <a href="#">1317</a>                                            |
| remote key server .....                          | <a href="#">1493</a>                                            |
| software-only platform .....                     | <a href="#">1321</a>                                            |
| subject names for an entity class .....          | <a href="#">1206</a>                                            |
| syslog server .....                              | <a href="#">1383</a>                                            |
| trunk group .....                                | <a href="#">784</a>                                             |
| vCenter to SDM .....                             | <a href="#">1378</a>                                            |
| Adding                                           |                                                                 |

|                                                                      |                          |
|----------------------------------------------------------------------|--------------------------|
| Adding ( <i>continued</i> )                                          |                          |
| administrative user .....                                            | <a href="#">76</a>       |
| listen-only .....                                                    | <a href="#">775</a>      |
| Service Observe .....                                                | <a href="#">775</a>      |
| so-coach .....                                                       | <a href="#">775</a>      |
| VOA Repeat .....                                                     | <a href="#">776</a>      |
| adding a CM Endpoint profile .....                                   | <a href="#">263</a>      |
| adding a contact in contact list .....                               | <a href="#">274</a>      |
| adding a CS 1000 profile .....                                       | <a href="#">269</a>      |
| Adding a data module                                                 |                          |
| data modules; adding .....                                           | <a href="#">805</a>      |
| adding additional certificate .....                                  | <a href="#">1190</a>     |
| adding agent .....                                                   | <a href="#">658</a>      |
| adding agents in bulk                                                |                          |
| agents; bulk add .....                                               | <a href="#">660</a>      |
| adding a local WebLM server .....                                    | <a href="#">1048</a>     |
| adding a messaging profile .....                                     | <a href="#">266</a>      |
| adding an announcement .....                                         | <a href="#">672</a>      |
| adding an audio group .....                                          | <a href="#">683</a>      |
| adding an element access profile .....                               | <a href="#">909</a>      |
| adding an entity class .....                                         | <a href="#">1200</a>     |
| adding an IP Office endpoint profile .....                           | <a href="#">271</a>      |
| adding announcements .....                                           | <a href="#">672</a>      |
| adding an SNMP Access profile .....                                  | <a href="#">904</a>      |
| adding an SNMP target profile .....                                  | <a href="#">960</a>      |
| adding a postal address of a private contact .....                   | <a href="#">282</a>      |
| adding a private contact .....                                       | <a href="#">280</a>      |
| adding a shared address .....                                        | <a href="#">605</a>      |
| adding a trunk group .....                                           | <a href="#">784</a>      |
| adding a trusted certificate to Communication Manager ..             | <a href="#">1500</a>     |
| Adding a UCM and Application Server Configuration template .....     | <a href="#">1150</a>     |
| adding audio groups .....                                            | <a href="#">683</a>      |
| adding a user address .....                                          | <a href="#">254</a>      |
| adding a vector routing table .....                                  | <a href="#">692</a>      |
| Adding a VMPro Call Flow template .....                              | <a href="#">1158</a>     |
| Adding a VMPro System Configuration template .....                   | <a href="#">1154</a>     |
| adding certificates                                                  |                          |
| available hosts .....                                                | <a href="#">1350</a>     |
| existing hosts .....                                                 | <a href="#">1350</a>     |
| migrated hosts .....                                                 | <a href="#">1350</a>     |
| adding CM Agent template .....                                       | <a href="#">1116</a>     |
| adding CM Endpoint template .....                                    | <a href="#">1118</a>     |
| Adding Communication Manager certificate to the System Manager ..... | <a href="#">1503</a>     |
| adding communication profile for user .....                          | <a href="#">258</a>      |
| adding communication profiles                                        |                          |
| IP Office endpoint .....                                             | <a href="#">271</a>      |
| Adding corporate logo .....                                          | <a href="#">74</a>       |
| adding coverage path                                                 |                          |
| coverage path; add .....                                             | <a href="#">698</a>      |
| adding coverage time-of-day                                          |                          |
| coverage time-of-day; add .....                                      | <a href="#">706</a>      |
| adding custom role .....                                             | <a href="#">187</a>      |
| adding dependencies to endpoints .....                               | <a href="#">833</a>      |
| adding endpoints .....                                               | <a href="#">712</a>      |
| adding ESXi host .....                                               | <a href="#">1319</a>     |
| adding hunt group .....                                              | <a href="#">780</a>      |
| adding IP Office endpoint template .....                             | <a href="#">1140</a>     |
| adding IP Office system configuration templates .....                | <a href="#">1144</a>     |
| adding location .....                                                | <a href="#">1317</a>     |
| adding location to host .....                                        | <a href="#">1380</a>     |
| adding new instance of element .....                                 | <a href="#">898</a>      |
| adding new users .....                                               | <a href="#">1290</a>     |
| adding OfficeLinx to System Manager .....                            | <a href="#">929</a>      |
| Adding off PBX endpoint mapping .....                                | <a href="#">789</a>      |
| adding Remote Servers .....                                          | <a href="#">1093</a>     |
| adding resources to a selected group .....                           | <a href="#">176</a>      |
| adding subnetworks .....                                             | <a href="#">908</a>      |
| adding subscriber templates                                          |                          |
| field descriptions .....                                             | <a href="#">1132</a>     |
| adding subscriber templates; field description .....                 | <a href="#">1135</a>     |
| adding subscriber templates MM; field description .....              | <a href="#">1137</a>     |
| adding synchronization datasources .....                             | <a href="#">82</a>       |
| adding templates                                                     |                          |
| subscriber .....                                                     | <a href="#">1121</a>     |
| adding trusted certificate                                           |                          |
| primary to secondary server .....                                    | <a href="#">108</a>      |
| secondary to primary server .....                                    | <a href="#">125</a>      |
| adding trusted certificates .....                                    | <a href="#">1184</a>     |
| WebLM .....                                                          | <a href="#">1048</a>     |
| adding UDP entries .....                                             | <a href="#">828</a>      |
| adding udp group .....                                               | <a href="#">823</a>      |
| adding uniform dial plan group .....                                 | <a href="#">823</a>      |
| adding Utility Services to System Manager .....                      | <a href="#">925</a>      |
| adding vCenter to SDM .....                                          | <a href="#">1378</a>     |
| adding vector directory number                                       |                          |
| vector directory number; add .....                                   | <a href="#">689</a>      |
| Add IP Office                                                        |                          |
| field description .....                                              | <a href="#">952</a>      |
| additional certificate                                               |                          |
| adding .....                                                         | <a href="#">1190</a>     |
| additional identity certificate                                      |                          |
| removing .....                                                       | <a href="#">1192</a>     |
| Additional Post Login Banner Message .....                           | <a href="#">73</a>       |
| Add local WebLM page .....                                           | <a href="#">1058</a>     |
| Add Mapping .....                                                    | <a href="#">196, 197</a> |
| Add new Administrative Users                                         |                          |
| field descriptions .....                                             | <a href="#">78</a>       |
| Add new Administrative Users field descriptions .....                | <a href="#">78</a>       |
| Add New Role .....                                                   | <a href="#">195, 196</a> |
| Add Platform .....                                                   | <a href="#">1343</a>     |
| add resources; selected groups .....                                 | <a href="#">176</a>      |
| address, deleting .....                                              | <a href="#">255</a>      |
| Add service to user .....                                            | <a href="#">615</a>      |
| add SNMP Access profile .....                                        | <a href="#">904</a>      |
| Add Station Template .....                                           | <a href="#">737</a>      |
| add subscribers                                                      |                          |
| Messaging field descriptions .....                                   | <a href="#">643</a>      |
| add System Platform .....                                            | <a href="#">923</a>      |
| Add To New Group .....                                               | <a href="#">176</a>      |
| administration                                                       |                          |
| Session Manager communication profile .....                          | <a href="#">260</a>      |
| administrative user                                                  |                          |

## Index

|                                                        |                      |                                                   |                                                                    |
|--------------------------------------------------------|----------------------|---------------------------------------------------|--------------------------------------------------------------------|
| administrative user ( <i>continued</i> )               |                      | alarms ( <i>continued</i> )                       |                                                                    |
| adding .....                                           | <a href="#">76</a>   | viewing .....                                     | <a href="#">991</a>                                                |
| editing details .....                                  | <a href="#">76</a>   | alarms; search .....                              | <a href="#">993</a>                                                |
| enabling .....                                         | <a href="#">77</a>   | Alarms for Conferencing .....                     | <a href="#">151</a>                                                |
| Administrative user                                    |                      | Alarms for IP Office .....                        | <a href="#">156</a>                                                |
| deleting .....                                         | <a href="#">77</a>   | alarm status                                      |                                                                    |
| editing roles .....                                    | <a href="#">76</a>   | changing .....                                    | <a href="#">991</a>                                                |
| viewing details .....                                  | <a href="#">75</a>   | alarm throttling; change .....                    | <a href="#">994</a>                                                |
| administrative user details                            |                      | alert message at login .....                      | <a href="#">51</a>                                                 |
| editing .....                                          | <a href="#">76</a>   | all announcements; backup .....                   | <a href="#">674</a>                                                |
| Administrative Users .....                             | <a href="#">220</a>  | all coverage paths .....                          | <a href="#">700</a>                                                |
| field descriptions .....                               | <a href="#">78</a>   | all endpoints .....                               | <a href="#">724</a>                                                |
| Administrative user sessions                           |                      | all hunt groups .....                             | <a href="#">782</a>                                                |
| terminating .....                                      | <a href="#">78</a>   | Allocations by Local WebLM .....                  | <a href="#">1066</a>                                               |
| Administrative Users field descriptions .....          | <a href="#">78</a>   | Allow access to Administrative Users Web UI ..... | <a href="#">220</a>                                                |
| administrator privilege                                |                      | all vector directory numbers .....                | <a href="#">691</a>                                                |
| login information .....                                | <a href="#">53</a>   | alternate source .....                            | <a href="#">1287</a>                                               |
| adopter application                                    |                      | upgrades .....                                    | <a href="#">1288</a>                                               |
| cannot communicate with WebLM .....                    | <a href="#">1045</a> | Always Use                                        |                                                                    |
| advanced search                                        |                      | Station .....                                     | <a href="#">749</a>                                                |
| searching announcements .....                          | <a href="#">678</a>  | analyze inventory                                 |                                                                    |
| searching endpoints .....                              | <a href="#">718</a>  | SDM .....                                         | <a href="#">1311</a> , <a href="#">1355</a>                        |
| Advance Options Presence Integration .....             | <a href="#">760</a>  | analyze job status .....                          | <a href="#">1436</a>                                               |
| AES                                                    |                      | analyze software .....                            | <a href="#">1444</a>                                               |
| user management .....                                  | <a href="#">157</a>  | analyzing                                         |                                                                    |
| agent                                                  |                      | software .....                                    | <a href="#">1445</a>                                               |
| adding dependencies .....                              | <a href="#">833</a>  | analyzing software inventory .....                | <a href="#">1451</a>                                               |
| Agent editor                                           |                      | announcement .....                                | <a href="#">670</a>                                                |
| permissions .....                                      | <a href="#">202</a>  | add .....                                         | <a href="#">672</a>                                                |
| Agent Management page .....                            | <a href="#">864</a>  | new .....                                         | <a href="#">672</a>                                                |
| agents .....                                           | <a href="#">658</a>  | Announcements                                     |                                                                    |
| download excel template .....                          | <a href="#">663</a>  | field descriptions .....                          | <a href="#">679</a>                                                |
| exporting all agents .....                             | <a href="#">662</a>  | announcements; backup .....                       | <a href="#">674</a>                                                |
| exporting selected agent .....                         | <a href="#">661</a>  | announcements; broadcast .....                    | <a href="#">676</a>                                                |
| field description .....                                | <a href="#">663</a>  | announcements; delete .....                       | <a href="#">673</a>                                                |
| importing agents .....                                 | <a href="#">662</a>  | announcements; download .....                     | <a href="#">674</a>                                                |
| agents; bulk delete .....                              | <a href="#">661</a>  | announcements; edit .....                         | <a href="#">672</a>                                                |
| agents field descriptions .....                        | <a href="#">663</a>  | announcements; filter .....                       | <a href="#">678</a>                                                |
| Agent Skill                                            |                      | announcements; move .....                         | <a href="#">675</a>                                                |
| Adding .....                                           | <a href="#">777</a>  | announcements; restore .....                      | <a href="#">675</a>                                                |
| SIP Phones .....                                       | <a href="#">777</a>  | announcements; save .....                         | <a href="#">673</a>                                                |
| agents list .....                                      | <a href="#">658</a>  | announcements; view .....                         | <a href="#">673</a>                                                |
| agent template                                         |                      | announcements list .....                          | <a href="#">670</a>                                                |
| field description .....                                | <a href="#">1126</a> | anonymous communication profiles .....            | <a href="#">984</a>                                                |
| agent template field description .....                 | <a href="#">1126</a> | anonymous profiles .....                          | <a href="#">982</a>                                                |
| Alarming .....                                         | <a href="#">990</a>  | assign .....                                      | <a href="#">982</a>                                                |
| Alarming UI .....                                      | <a href="#">878</a>  | delete .....                                      | <a href="#">982</a>                                                |
| Alarm List page .....                                  | <a href="#">999</a>  | answer .....                                      | <a href="#">771</a>                                                |
| alarms                                                 |                      | appender; modify .....                            | <a href="#">1020</a>                                               |
| CS 1000 .....                                          | <a href="#">139</a>  | Appliance Virtualization Host                     |                                                                    |
| delete .....                                           | <a href="#">992</a>  | configure login banner .....                      | <a href="#">1338</a>                                               |
| exclude .....                                          | <a href="#">962</a>  | push login banner .....                           | <a href="#">1338</a>                                               |
| exporting .....                                        | <a href="#">992</a>  | Appliance Virtualization Platform .....           | <a href="#">1324</a> , <a href="#">1332</a> , <a href="#">1345</a> |
| forward from secondary to primary System Manager ..... | <a href="#">996</a>  | change password .....                             | <a href="#">1328</a>                                               |
| include .....                                          | <a href="#">962</a>  | generating kickstart file .....                   | <a href="#">1328</a>                                               |
| remote key server .....                                | <a href="#">991</a>  | license file .....                                | <a href="#">1334</a>                                               |
| standby mode .....                                     | <a href="#">997</a>  | push syslog .....                                 | <a href="#">1384</a>                                               |

|                                                                                  |                                             |
|----------------------------------------------------------------------------------|---------------------------------------------|
| Appliance Virtualization Platform ( <i>continued</i> )                           |                                             |
| restarting .....                                                                 | <a href="#">1337</a>                        |
| shutting down .....                                                              | <a href="#">1337</a>                        |
| update .....                                                                     | <a href="#">1347</a>                        |
| WebLM Configuration .....                                                        | <a href="#">1334</a>                        |
| Appliance Virtualization Platform host Gateway                                   |                                             |
| change .....                                                                     | <a href="#">1323</a>                        |
| edit .....                                                                       | <a href="#">1323</a>                        |
| Appliance Virtualization Platform host IP address                                |                                             |
| change .....                                                                     | <a href="#">1323</a>                        |
| edit .....                                                                       | <a href="#">1323</a>                        |
| Appliance Virtualization Platform host password                                  |                                             |
| changing .....                                                                   | <a href="#">1327</a>                        |
| Appliance Virtualization Platform network parameters .....                       | <a href="#">1323</a>                        |
| application                                                                      |                                             |
| deleting .....                                                                   | <a href="#">1359</a>                        |
| edit .....                                                                       | <a href="#">1358</a>                        |
| monitoring .....                                                                 | <a href="#">1377</a>                        |
| re-establishing trust .....                                                      | <a href="#">1356</a>                        |
| restart .....                                                                    | <a href="#">1361</a>                        |
| start .....                                                                      | <a href="#">1360</a>                        |
| stop .....                                                                       | <a href="#">1361</a>                        |
| Application Deployment                                                           |                                             |
| field descriptions .....                                                         | <a href="#">1364</a>                        |
| application instance                                                             |                                             |
| create .....                                                                     | <a href="#">898</a>                         |
| new .....                                                                        | <a href="#">898</a>                         |
| application instances .....                                                      | <a href="#">896</a>                         |
| Application management .....                                                     | <a href="#">1316</a>                        |
| application management page .....                                                | <a href="#">78</a> , <a href="#">933</a>    |
| applications                                                                     |                                             |
| preupgrade check .....                                                           | <a href="#">1314</a>                        |
| Applications .....                                                               | <a href="#">1386</a>                        |
| applying                                                                         |                                             |
| third-party certificates to Appliance Virtualization Platform .....              | <a href="#">1210</a> , <a href="#">1339</a> |
| Applying a Communication Manager patch .....                                     | <a href="#">1485</a>                        |
| Applying an IP Office system configuration template on an IP Office device ..... | <a href="#">1146</a>                        |
| Applying a UCM and Application Server Configuration template .....               | <a href="#">1153</a>                        |
| Applying a VMPro call flow template on a device .....                            | <a href="#">1160</a>                        |
| Applying a VMPro System Configuration template on a device .....                 | <a href="#">1156</a>                        |
| Argument .....                                                                   | <a href="#">756</a>                         |
| Assertions .....                                                                 | <a href="#">1246</a>                        |
| assign                                                                           |                                             |
| tenant administrator .....                                                       | <a href="#">1259</a>                        |
| assigned elements                                                                |                                             |
| remove .....                                                                     | <a href="#">920</a>                         |
| assigned resources                                                               |                                             |
| remove .....                                                                     | <a href="#">167</a>                         |
| assign groups                                                                    |                                             |
| multiple users .....                                                             | <a href="#">251</a> , <a href="#">252</a>   |
| single user .....                                                                | <a href="#">251</a>                         |
| Assign Groups .....                                                              | <a href="#">366</a>                         |
| assign groups to user .....                                                      | <a href="#">366</a>                         |
| assigning                                                                        |                                             |
| shared address to user .....                                                     | <a href="#">255</a> , <a href="#">604</a>   |
| assigning an appender to a logger .....                                          | <a href="#">1019</a>                        |
| assigning anonymous profiles .....                                               | <a href="#">982</a>                         |
| assigning applications .....                                                     | <a href="#">919</a>                         |
| assigning filter profile to serviceability agent .....                           | <a href="#">964</a>                         |
| Assigning permissions                                                            |                                             |
| CM templates .....                                                               | <a href="#">1120</a>                        |
| assigning permissions in user management .....                                   | <a href="#">202</a>                         |
| assigning permissions through User Management .....                              | <a href="#">202</a>                         |
| assigning permission to access UDP groups .....                                  | <a href="#">830</a>                         |
| assigning range for endpoints .....                                              | <a href="#">209</a>                         |
| assigning resources .....                                                        | <a href="#">176</a>                         |
| assigning resources to group .....                                               | <a href="#">163</a>                         |
| assigning roles to                                                               |                                             |
| multiple users .....                                                             | <a href="#">250</a>                         |
| assigning users to role .....                                                    | <a href="#">192</a>                         |
| assign permissions in Scheduler .....                                            | <a href="#">1097</a>                        |
| assign permissions in Solution Deployment Manager .....                          | <a href="#">190</a>                         |
| Assign Role page .....                                                           | <a href="#">365</a>                         |
| Assign Roles page .....                                                          | <a href="#">364</a>                         |
| assign roles to                                                                  |                                             |
| single user .....                                                                | <a href="#">249</a>                         |
| assign users .....                                                               | <a href="#">192</a> , <a href="#">253</a>   |
| Assign Users .....                                                               | <a href="#">197</a> , <a href="#">368</a>   |
| assign users to role .....                                                       | <a href="#">192</a>                         |
| assign users to roles .....                                                      | <a href="#">253</a>                         |
| association between IP Office endpoint profile and user                          |                                             |
| remove .....                                                                     | <a href="#">274</a>                         |
| asymmetric keys                                                                  |                                             |
| regenerating .....                                                               | <a href="#">1252</a>                        |
| Attach Appender page .....                                                       | <a href="#">1022</a>                        |
| attach contacts page .....                                                       | <a href="#">276</a>                         |
| Attendant                                                                        |                                             |
| New Endpoint .....                                                               | <a href="#">739</a>                         |
| attribute details defined in Delete user XSD .....                               | <a href="#">535</a>                         |
| attribute details defined in Import User XSD .....                               | <a href="#">524</a>                         |
| attribute details defined in the CM Endpoint profile XSD .....                   | <a href="#">536</a>                         |
| attribute details defined in the Conferencing communication profile XSD .....    | <a href="#">579</a>                         |
| attribute details defined in the Messaging communication profile XSD .....       | <a href="#">565</a>                         |
| attribute details defined in the Session Manager communication profile XSD ..... | <a href="#">574</a>                         |
| Audible Message Waiting .....                                                    | <a href="#">749</a>                         |
| audio groups .....                                                               | <a href="#">682</a>                         |
| audio groups; add .....                                                          | <a href="#">683</a>                         |
| audio groups; delete .....                                                       | <a href="#">684</a>                         |
| audio groups; edit .....                                                         | <a href="#">683</a>                         |
| audio groups; more actions .....                                                 | <a href="#">684</a>                         |
| audio groups; view .....                                                         | <a href="#">683</a>                         |
| audio groups field description .....                                             | <a href="#">684</a>                         |
| audit logging                                                                    |                                             |
| configuring .....                                                                | <a href="#">1029</a>                        |
| audit logging configuration                                                      |                                             |
| field descriptions .....                                                         | <a href="#">1029</a>                        |
| audit logging configuration field descriptions .....                             | <a href="#">1029</a>                        |

|                                                         |                                             |                                                                           |                                           |
|---------------------------------------------------------|---------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------|
| audit reports .....                                     | <a href="#">979</a>                         | Backing up Communication Manager or Communication Manager Messaging ..... | <a href="#">1465</a>                      |
| Audix Name .....                                        | <a href="#">747</a>                         | backup .....                                                              | <a href="#">838</a> , <a href="#">840</a> |
| authentication                                          |                                             | remote server .....                                                       | <a href="#">843</a>                       |
| Kerberos server .....                                   | <a href="#">1242</a>                        | backup and restore .....                                                  | <a href="#">838</a> , <a href="#">840</a> |
| authentication scheme                                   |                                             | Backup and Restore page .....                                             | <a href="#">853</a>                       |
| edit .....                                              | <a href="#">1240</a>                        | backup and restore service; access .....                                  | <a href="#">841</a>                       |
| authentication servers                                  |                                             | backup and restore time .....                                             | <a href="#">851</a>                       |
| field descriptions .....                                | <a href="#">1243</a>                        | backup encryption                                                         |                                           |
| provisioning .....                                      | <a href="#">1241</a>                        | enabling .....                                                            | <a href="#">842</a>                       |
| authentication servers field descriptions .....         | <a href="#">1243</a>                        | Backup field descriptions .....                                           | <a href="#">853</a>                       |
| authorization code .....                                | <a href="#">817</a>                         | backup files; view .....                                                  | <a href="#">841</a>                       |
| authorization code field description                    |                                             | backup file size .....                                                    | <a href="#">850</a>                       |
| authorization code; field description .....             | <a href="#">819</a>                         | backup of announcements .....                                             | <a href="#">674</a>                       |
| authorization code list .....                           | <a href="#">818</a>                         | bidirectional synchronization .....                                       | <a href="#">80</a>                        |
| auto .....                                              | <a href="#">771</a>                         | Bindings .....                                                            | <a href="#">1246</a>                      |
| Auto activation of serviceability agents .....          | <a href="#">967</a>                         | Bridged Appearance Origination Restriction .....                          | <a href="#">753</a>                       |
| Auto answer .....                                       | <a href="#">771</a>                         | Bridged Call Alerting .....                                               | <a href="#">740</a>                       |
| field descriptions .....                                | <a href="#">772</a>                         | Bridged Idle Line Preference .....                                        | <a href="#">750</a>                       |
| Auto Answer                                             |                                             | broadcasting an announcement .....                                        | <a href="#">676</a>                       |
| Station .....                                           | <a href="#">741</a>                         | broadcasting announcements .....                                          | <a href="#">676</a>                       |
| automatic alternate routing digit conversion ,          |                                             | Building                                                                  |                                           |
| aar digit conversion .....                              | <a href="#">796</a> , <a href="#">798</a>   | Station .....                                                             | <a href="#">754</a>                       |
| ars digit conversion .....                              | <a href="#">796</a> , <a href="#">798</a>   | built-in roles .....                                                      | <a href="#">182</a>                       |
| automatic route selection digit conversion .....        | <a href="#">796</a> , <a href="#">798</a>   | Built-in roles .....                                                      | <a href="#">181</a>                       |
| automatic call routes                                   |                                             | bulk add endpoint; field descriptions .....                               | <a href="#">769</a>                       |
| using .....                                             | <a href="#">264</a>                         | bulk delete endpoints .....                                               | <a href="#">717</a>                       |
| automatic route selection toll,                         |                                             | bulk deleting agents .....                                                | <a href="#">661</a>                       |
| ars toll .....                                          | <a href="#">801</a>                         | bulk deleting endpoints .....                                             | <a href="#">717</a>                       |
| automatic route selection toll field descriptions ..... | <a href="#">802</a>                         | bulk edit                                                                 |                                           |
| automatic route selection toll list .....               | <a href="#">801</a>                         | users .....                                                               | <a href="#">233</a> , <a href="#">235</a> |
| AutoRefresh Alarm List page .....                       | <a href="#">997</a>                         | bulk export .....                                                         | <a href="#">370</a> , <a href="#">376</a> |
| auto-refresh log list page .....                        | <a href="#">1028</a>                        | key features .....                                                        | <a href="#">376</a>                       |
| Auto Select Any Idle Appearance .....                   | <a href="#">749</a>                         | bulk export of global user settings .....                                 | <a href="#">403</a>                       |
| Avaya Aura application                                  |                                             | bulk export of users .....                                                | <a href="#">383</a>                       |
| Services Port static routing update .....               | <a href="#">1360</a>                        | bulk export of users partially .....                                      | <a href="#">393</a>                       |
| Avaya Aura application upgrade .....                    | <a href="#">1393</a> , <a href="#">1402</a> | bulk export users .....                                                   | <a href="#">382</a>                       |
| Avaya Aura Conferencing configuration .....             | <a href="#">148</a>                         | bulk export utility .....                                                 | <a href="#">917</a>                       |
| Avaya Equinox Management                                |                                             | bulk import .....                                                         | <a href="#">370</a> , <a href="#">376</a> |
| SSO configuration .....                                 | <a href="#">153</a>                         | global settings options .....                                             | <a href="#">401</a>                       |
| Avaya Multimedia Messaging .....                        | <a href="#">158</a>                         | global user settings .....                                                | <a href="#">402</a>                       |
| Avaya SIP AST endpoints .....                           | <a href="#">1263</a>                        | key features .....                                                        | <a href="#">376</a>                       |
| Avaya support website .....                             | <a href="#">1537</a>                        | bulk import and export .....                                              | <a href="#">370</a> , <a href="#">376</a> |
| AVP_Bulk_Import                                         |                                             | bulk import and export of user by using Excel file .....                  | <a href="#">372</a>                       |
| bulk_import .....                                       | <a href="#">1419</a>                        | bulk import and export with Excel .....                                   | <a href="#">370</a>                       |
| sample scenario .....                                   | <a href="#">1419</a>                        | BulkImportEncryptionUtil .....                                            | <a href="#">394</a> , <a href="#">395</a> |
| AVP license status .....                                | <a href="#">1336</a>                        | bulk import encryption utility .....                                      | <a href="#">394</a>                       |
|                                                         |                                             | Bulk import of elements .....                                             | <a href="#">898</a>                       |
| <b>B</b>                                                |                                             | bulk import of global user settings .....                                 | <a href="#">401</a> , <a href="#">402</a> |
| B5800 endpoint templates                                |                                             | bulk import of partial user attributes .....                              | <a href="#">392</a>                       |
| duplicate .....                                         | <a href="#">1142</a>                        | bulk import of users .....                                                | <a href="#">379</a>                       |
| backing up all announcements .....                      | <a href="#">674</a>                         | bulk import users .....                                                   | <a href="#">377</a>                       |
| backing up audio groups .....                           | <a href="#">684</a>                         | bulk import XML for users with SIP phone .....                            | <a href="#">589</a>                       |
| backing up audio groups; field description .....        | <a href="#">684</a>                         | bulk user                                                                 |                                           |
| Backing up Communication Manager                        |                                             | delete .....                                                              | <a href="#">234</a>                       |
| Backing up Communication Manager Messaging ....         | <a href="#">1465</a>                        | bulk user edit job                                                        |                                           |
|                                                         |                                             | view .....                                                                | <a href="#">233</a>                       |



|                                                   |                                             |                                                           |                                             |
|---------------------------------------------------|---------------------------------------------|-----------------------------------------------------------|---------------------------------------------|
| Bulk User Editor .....                            | <a href="#">235</a>                         | certificate update ( <i>continued</i> )                   |                                             |
| Busy                                              |                                             | ESXi host .....                                           | <a href="#">1349</a>                        |
| Coverage Path .....                               | <a href="#">703</a>                         | vCenter .....                                             | <a href="#">1349</a>                        |
| Button Assignment .....                           | <a href="#">756</a>                         | VMware documentation .....                                | <a href="#">1349</a>                        |
| Button Feature .....                              | <a href="#">756</a>                         | certificate using CSR                                     |                                             |
| Button Label .....                                | <a href="#">756</a>                         | create .....                                              | <a href="#">1214</a>                        |
| <b>C</b>                                          |                                             | Certification                                             |                                             |
| Cable .....                                       | <a href="#">754</a>                         | validation .....                                          | <a href="#">1347</a>                        |
| CA certificate exchange                           |                                             | Certification validation .....                            | <a href="#">1347</a>                        |
| Avaya Equinox Management and System Manager ..... | <a href="#">152</a>                         | change                                                    |                                             |
| Call Appearance Display Format .....              | <a href="#">747</a>                         | Appliance Virtualization Platform host IP address ....    | <a href="#">1323</a>                        |
| Call Forwarding .....                             | <a href="#">756</a>                         | Host/ IP Settings .....                                   | <a href="#">1324</a>                        |
| cancel                                            |                                             | network settings .....                                    | <a href="#">1345</a>                        |
| global user settings import job .....             | <a href="#">407</a>                         | Network Settings .....                                    | <a href="#">1324</a>                        |
| cancel a global user settings import job .....    | <a href="#">407</a>                         | change abbreviated-dialing enhanced .....                 | <a href="#">755</a>                         |
| cancel a user import job .....                    | <a href="#">399</a>                         | change communication profile password .....               | <a href="#">223</a>                         |
| cancelling                                        |                                             | change FQDN                                               |                                             |
| endpoint migration job .....                      | <a href="#">732</a>                         | primary System Manager .....                              | <a href="#">1513</a>                        |
| capabilities                                      |                                             | change FQDN in the primary System Manager .....           | <a href="#">1513</a>                        |
| Solution Deployment Manager client .....          | <a href="#">1278</a> , <a href="#">1283</a> | change FQDN on primary System Manager .....               | <a href="#">1514</a>                        |
| System Manager Solution Deployment Manager ....   | <a href="#">1278</a>                        | change FQDN on secondary System Manager ....              | <a href="#">1515</a> , <a href="#">1516</a> |
| capability comparison                             |                                             | Change Gateway .....                                      | <a href="#">1344</a>                        |
| System Manager Solution Deployment Manager and    |                                             | change H323 and SIP passwords .....                       | <a href="#">221</a>                         |
| client capabilities .....                         | <a href="#">1278</a>                        | change IP address                                         |                                             |
| CDR Privacy .....                                 | <a href="#">750</a>                         | primary System Manager .....                              | <a href="#">1513</a>                        |
| centralized licensing .....                       | <a href="#">1039</a>                        | change IP address and FQDN on primary and secondary       |                                             |
| adding elements .....                             | <a href="#">1041</a>                        | System Manager .....                                      | <a href="#">1513</a>                        |
| disable .....                                     | <a href="#">1044</a>                        | change IP address for AVP host .....                      | <a href="#">1323</a>                        |
| enable .....                                      | <a href="#">1040</a>                        | change IP address on primary System Manager .....         | <a href="#">1513</a>                        |
| overview .....                                    | <a href="#">1039</a>                        | Change IP address on primary System Manager .....         | <a href="#">1514</a>                        |
| certificate                                       |                                             | change IP address on secondary System Manager             |                                             |
| authentication .....                              | <a href="#">54</a>                          | .....                                                     | <a href="#">1515</a> , <a href="#">1516</a> |
| generation capabilities .....                     | <a href="#">1178</a>                        | Change IP FQDN .....                                      | <a href="#">1358</a>                        |
| management capabilities .....                     | <a href="#">1178</a>                        | changeIPFQDN command, .....                               | <a href="#">1510</a>                        |
| Microsoft Active Directory .....                  | <a href="#">1183</a>                        | change Netmask for Appliance Virtualization Platform host |                                             |
| view .....                                        | <a href="#">1215</a>                        | .....                                                     | <a href="#">1323</a>                        |
| Certificate authorities .....                     | <a href="#">1209</a>                        | Change Network Params .....                               | <a href="#">1323</a>                        |
| Certificate Authority .....                       | <a href="#">1224</a>                        | Change Password page .....                                | <a href="#">53</a>                          |
| certificate-based authentication                  |                                             | changing                                                  |                                             |
| overview .....                                    | <a href="#">54</a>                          | alarm status .....                                        | <a href="#">991</a>                         |
| Certificate Enrollment .....                      | <a href="#">1214</a>                        | DNS .....                                                 | <a href="#">1509</a>                        |
| certificate generation .....                      | <a href="#">1212</a>                        | encryption passphrase .....                               | <a href="#">1491</a>                        |
| certificate keystore                              |                                             | FQDN .....                                                | <a href="#">1509</a>                        |
| generate .....                                    | <a href="#">1213</a>                        | Gateway .....                                             | <a href="#">1509</a>                        |
| certificate response .....                        | <a href="#">1226</a>                        | IP address .....                                          | <a href="#">1509</a>                        |
| certificates                                      |                                             | IP address and default gateway .....                      | <a href="#">1333</a>                        |
| accepting .....                                   | <a href="#">1348</a>                        | Netmask .....                                             | <a href="#">1509</a>                        |
| generating .....                                  | <a href="#">1348</a>                        | password policy through CLI .....                         | <a href="#">66</a>                          |
| revoking .....                                    | <a href="#">1199</a>                        | search list .....                                         | <a href="#">1509</a>                        |
| unrevoking .....                                  | <a href="#">1199</a>                        | System Manager TLS version .....                          | <a href="#">1168</a>                        |
| viewing .....                                     | <a href="#">1197</a>                        | changing allocations of a licensed feature .....          | <a href="#">1053</a>                        |
| certificate signing request .....                 | <a href="#">1224</a>                        | changing a managed element's FQDN .....                   | <a href="#">1512</a>                        |
| Certificate Signing Request                       |                                             | changing a managed element's IP address in System         |                                             |
| create .....                                      | <a href="#">1212</a>                        | Manager .....                                             | <a href="#">1512</a>                        |
| certificate update                                |                                             | changing compatibility view setting .....                 | <a href="#">45</a>                          |
|                                                   |                                             | changing System Manager IP address in managed elements    |                                             |
|                                                   |                                             | .....                                                     | <a href="#">1512</a>                        |

|                                                                        |          |                                                          |                              |
|------------------------------------------------------------------------|----------|----------------------------------------------------------|------------------------------|
| changing the Appliance Virtualization Platform host password .....     | 1327     | CM audit report field descriptions .....                 | 980                          |
| changing the TLS version of primary and secondary System Manager ..... | 1169     | CM Endpoint profile .....                                |                              |
| changing to classic view .....                                         | 657      | delete .....                                             | 265                          |
| Check .....                                                            | 1448     | CM Endpoint template .....                               |                              |
| checking .....                                                         |          | upgrade .....                                            | 1115                         |
| backup failure .....                                                   | 839      | CM Endpoint templates .....                              |                              |
| checklist .....                                                        |          | add .....                                                | 1118                         |
| Branch Session Manager upgrade .....                                   | 1394     | copy .....                                               | 1120                         |
| Communication Manager 6.x upgrade .....                                | 1453     | delete .....                                             | 1119                         |
| Session Manager upgrade .....                                          | 1394     | edit .....                                               | 1118                         |
| Choose Address page .....                                              | 257      | view .....                                               | 1119                         |
| choose a shared address for a private contact .....                    | 596      | CM notify .....                                          |                              |
| Choose Group page .....                                                | 180      | configure two-way TLS .....                              | 1503                         |
| choose parent group .....                                              | 180      | CM notify sync feature .....                             | 1497                         |
| choosing .....                                                         |          | CM objetscs .....                                        | 652                          |
| shared address .....                                                   | 255, 604 | CM station data .....                                    |                              |
| choosing a shared address for a private contact .....                  | 284      | export .....                                             | 370                          |
| cipher suite list .....                                                | 1168     | import .....                                             | 370                          |
| class of service .....                                                 | 814      | CM templates .....                                       |                              |
| messaging .....                                                        | 639      | permissions .....                                        | 1120                         |
| Class of Service .....                                                 |          | CM Upgrade Configuration .....                           |                              |
| COS List .....                                                         | 640      | field description .....                                  | 1466                         |
| class of service data; edit .....                                      | 814      | collecting inventory .....                               | 1443                         |
| class of service data; view .....                                      | 814      | collection .....                                         |                              |
| class of service field description .....                               | 815      | delete .....                                             | 1535                         |
| class of service group, .....                                          |          | edit name .....                                          | 1535                         |
| cos group .....                                                        | 819      | generating PDF .....                                     | 1535                         |
| system; class of service group .....                                   | 819      | sharing content .....                                    | 1535                         |
| class of service group field descriptions .....                        |          | command .....                                            |                              |
| class of service group; field description .....                        | 821      | changeIPFQDN .....                                       | 1510                         |
| class of service group list .....                                      | 819      | configureOutboundFirewall .....                          | 1171                         |
| class of service list; field description .....                         | 815      | configureTimeZone .....                                  | 1530                         |
| class of service list; filter .....                                    | 814      | exportUpmGlobalsettings .....                            | 403                          |
| CleanUp .....                                                          | 983      | logRetention .....                                       | 862                          |
| clean up communication profiles .....                                  | 983      | manageEntityClassWhitelist .....                         | 1204                         |
| CLI .....                                                              |          | outboundConnectionLogging .....                          | 1170                         |
| SSH .....                                                              | 57       | pruneAllLogs.sh .....                                    | 863                          |
| CLI access .....                                                       |          | runRTSCli.sh .....                                       | 918                          |
| certificate-based .....                                                | 56       | setSecurityPolicy .....                                  | 64                           |
| client audit .....                                                     | 1071     | updateLogRetention.sh .....                              | 863                          |
| Client node locking .....                                              | 1034     | command line restore .....                               | 849                          |
| client Solution Deployment Manager .....                               | 1276     | command runRTSCli.sh .....                               | 917                          |
| cluster level alarming .....                                           | 990      | common causes .....                                      |                              |
| Cluster Session Manager .....                                          | 802      | application deployment failure .....                     | 1363                         |
| CM Agent template .....                                                |          | communication address .....                              |                              |
| upgrade .....                                                          | 1115     | modifying .....                                          | 259                          |
| view .....                                                             | 1117     | Communication Manager .....                              |                              |
| CM Agent template; .....                                               |          | 6.3.100 .....                                            | 1440                         |
| add .....                                                              | 1116     | adding .....                                             | 926                          |
| copy .....                                                             | 1117     | Multi Tenancy .....                                      | 1264                         |
| delete .....                                                           | 1117     | upgrade .....                                            | 1440                         |
| edit .....                                                             | 1116     | Communication Manager; adding a trusted certificate .... | 1500                         |
| CM audit .....                                                         | 979      | Communication Manager; update .....                      | 1485                         |
| CM audit field description .....                                       | 979      | Communication Manager 5.2.1 .....                        |                              |
| CM audit report; field description .....                               | 980      | upgrade .....                                            | 1455, 1464, 1472, 1475, 1476 |
|                                                                        |          | upgrade on different server .....                        | 1474                         |
|                                                                        |          | Communication Manager 5.2.1 to 6.3.100 upgrade .....     | 1476                         |

|                                                          |                                                                    |                                                           |                                           |
|----------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------------|-------------------------------------------|
| Communication Manager 5.2.1 upgrade .....                | <a href="#">1463</a>                                               | completed jobs ( <i>continued</i> ) .....                 |                                           |
| Communication Manager 5.x upgrade .....                  | <a href="#">1484</a>                                               | view .....                                                | <a href="#">1099</a>                      |
| Communication Manager 6.x .....                          | <a href="#">1453</a>                                               | Completed Jobs Page .....                                 | <a href="#">1105</a>                      |
| upgrade .....                                            | <a href="#">1456</a> , <a href="#">1457</a>                        | Conf/Trans On Primary Appearance .....                    | <a href="#">750</a>                       |
| Communication Manager audit .....                        | <a href="#">979</a>                                                | Conferencing configuration .....                          | <a href="#">148</a>                       |
| Communication Manager Backup Configuration field         |                                                                    | Conferencing GR configuration .....                       | <a href="#">148</a>                       |
| descriptions .....                                       | <a href="#">1466</a>                                               | configuration .....                                       | <a href="#">379</a> , <a href="#">391</a> |
| Communication Manager capabilities .....                 | <a href="#">648</a>                                                | Conferencing .....                                        | <a href="#">148</a>                       |
| Communication Manager configuration when primary System  |                                                                    | IP Phone Group ID .....                                   | <a href="#">747</a>                       |
| Manager is nonoperational .....                          | <a href="#">138</a>                                                | Meeting Exchange element .....                            | <a href="#">143</a>                       |
| Communication Manager data .....                         | <a href="#">972</a>                                                | Messaging .....                                           | <a href="#">144</a>                       |
| Communication Manager notify sync .....                  | <a href="#">1497</a>                                               | syslog server .....                                       | <a href="#">1383</a>                      |
| Communication Manager objects .....                      | <a href="#">652</a>                                                | Configuration and Network Parameters .....                |                                           |
| Communication Manager objects; add .....                 |                                                                    | AVP Utilities .....                                       | <a href="#">1369</a>                      |
| adding Communication Manager objects .....               | <a href="#">655</a>                                                | Communication Manager .....                               | <a href="#">1364</a>                      |
| Communication Manager objects; changing to classic view  |                                                                    | Communication Manager Messaging .....                     | <a href="#">1369</a>                      |
| .....                                                    | <a href="#">657</a>                                                | configuration management .....                            | <a href="#">864</a>                       |
| Communication Manager objects; delete .....              |                                                                    | configuration options for bulk import of users .....      | <a href="#">391</a>                       |
| deleting Communication Manager objects .....             | <a href="#">656</a>                                                | configuration options for bulk import through Excel ..... | <a href="#">379</a>                       |
| Communication Manager objects; edit .....                |                                                                    | configure .....                                           |                                           |
| Communication Manager objects; edit .....                | <a href="#">656</a>                                                | Communication Manager when primary System Manager         |                                           |
| Communication Manager Session Manager correlation .....  | <a href="#">836</a>                                                | is nonoperational .....                                   | <a href="#">138</a>                       |
| Communication Manager templates .....                    |                                                                    | Geographical Redundancy .....                             | <a href="#">117</a>                       |
| permissions .....                                        | <a href="#">1120</a>                                               | health monitoring timeout interval .....                  | <a href="#">120</a>                       |
| Communication Manager update .....                       | <a href="#">1357</a> , <a href="#">1397</a> , <a href="#">1399</a> | Hosted Service Provider on System Manager .....           | <a href="#">1248</a>                      |
| Communication Manager upgrade from Software              |                                                                    | login banner on host .....                                | <a href="#">1338</a>                      |
| Management .....                                         | <a href="#">1392</a>                                               | Remote Identity Provider .....                            | <a href="#">1248</a>                      |
| Communication Manager upgrade from System Manager        |                                                                    | configure alarm throttling .....                          | <a href="#">994</a>                       |
| .....                                                    | <a href="#">1392</a>                                               | configure centralized licensing .....                     | <a href="#">1040</a>                      |
| Communication Manager upgrades .....                     | <a href="#">1439</a>                                               | field description .....                                   | <a href="#">1040</a>                      |
| communication profile .....                              |                                                                    | field descriptions .....                                  | <a href="#">1040</a>                      |
| adding .....                                             | <a href="#">258</a>                                                | configure Conferencing .....                              | <a href="#">151</a>                       |
| CM Endpoint profile for a user .....                     | <a href="#">262</a>                                                | configure CS 1000 SNMP alarms .....                       | <a href="#">139</a>                       |
| Messaging profile for a user .....                       | <a href="#">266</a>                                                | configure customized interface .....                      |                                           |
| Presence .....                                           | <a href="#">262</a>                                                | field descriptions .....                                  | <a href="#">74</a>                        |
| Communication profile .....                              | <a href="#">295</a>                                                | configure enterprise licensing .....                      | <a href="#">1046</a>                      |
| communication profile for a user .....                   |                                                                    | configure FTP server as remote server .....               | <a href="#">1296</a>                      |
| deleting .....                                           | <a href="#">258</a>                                                | configureNTP .....                                        | <a href="#">1530</a>                      |
| communication profile password history policy .....      | <a href="#">609</a>                                                | Configure options .....                                   | <a href="#">988</a>                       |
| communication profile password policy .....              |                                                                    | Configure Presence Server .....                           | <a href="#">143</a>                       |
| edit .....                                               | <a href="#">610</a>                                                | configure remote server .....                             |                                           |
| Communication Profile Password Policy field descriptions | <a href="#">611</a>                                                | protocol support .....                                    | <a href="#">1294</a>                      |
| communication profile password strength policy .....     | <a href="#">609</a>                                                | configure revocation information in SubCA .....           | <a href="#">1227</a>                      |
| communication profiles .....                             | <a href="#">257</a>                                                | configureTimeZone .....                                   | <a href="#">1530</a>                      |
| clean up .....                                           | <a href="#">983</a>                                                | configuring .....                                         |                                           |
| delete .....                                             | <a href="#">983</a>                                                | audit logging .....                                       | <a href="#">1029</a>                      |
| communication profiles; synchronize .....                | <a href="#">980</a>                                                | Avaya Services registration .....                         | <a href="#">931</a>                       |
| communication profiles synchronization .....             | <a href="#">980</a>                                                | cipher suite list on System Manager .....                 | <a href="#">1168</a>                      |
| communication profile worksheets .....                   |                                                                    | CRL download .....                                        | <a href="#">1234</a>                      |
| communication profile hierarchy .....                    | <a href="#">374</a>                                                | email properties .....                                    | <a href="#">1091</a>                      |
| hierarchy .....                                          | <a href="#">374</a>                                                | Geographical Redundancy .....                             | <a href="#">109</a>                       |
| parent-child communication profile .....                 | <a href="#">374</a>                                                | IP Phone Group ID .....                                   | <a href="#">748</a>                       |
| relationship .....                                       | <a href="#">374</a>                                                | Multimedia Messaging .....                                | <a href="#">158</a>                       |
| worksheets .....                                         | <a href="#">374</a>                                                | outbound firewall rule .....                              | <a href="#">1173</a>                      |
| Company ID .....                                         | <a href="#">1288</a>                                               | periodic report cleanup .....                             | <a href="#">1092</a>                      |
| compatibility mode .....                                 | <a href="#">45</a>                                                 | report properties .....                                   | <a href="#">1092</a>                      |
| completed jobs .....                                     | <a href="#">1100</a>                                               | SAL Gateway .....                                         | <a href="#">930</a>                       |

|                                                                                                  |                                             |
|--------------------------------------------------------------------------------------------------|---------------------------------------------|
| configuring ( <i>continued</i> )                                                                 |                                             |
| System Manager as local software library .....                                                   | <a href="#">1294</a>                        |
| WebLM Server on Appliance Virtualization Platform .....                                          | <a href="#">1335</a>                        |
| Configuring                                                                                      |                                             |
| GR-unaware elements .....                                                                        | <a href="#">131</a>                         |
| configuring audit logging .....                                                                  | <a href="#">1029</a>                        |
| Configuring Communication Manager during GR failback .....                                       | <a href="#">137</a>                         |
| Configuring Communication Manager during GR failover .....                                       | <a href="#">136</a>                         |
| Configuring Communication Manager during GR failover<br>when only the primary is reachable ..... | <a href="#">138</a>                         |
| configuring communication manager user profile settings .....                                    | <a href="#">649</a>                         |
| Configuring Conferencing to be managed by System<br>Manager .....                                | <a href="#">148</a>                         |
| Configuring CS 1000 .....                                                                        | <a href="#">139</a>                         |
| Configuring DTLS for CS 1000 .....                                                               | <a href="#">1233</a>                        |
| configuring EASG                                                                                 |                                             |
| during G430 and G450 Branch Gateway upgrade ...                                                  | <a href="#">1482</a>                        |
| gateway .....                                                                                    | <a href="#">1482</a>                        |
| configuring endpoints .....                                                                      | <a href="#">831</a>                         |
| configuringfor GR                                                                                |                                             |
| IP Office .....                                                                                  | <a href="#">154</a>                         |
| configuring IP Office .....                                                                      | <a href="#">865</a>                         |
| field description .....                                                                          | <a href="#">865</a>                         |
| configuring IP Office in Active-Active scenario .....                                            | <a href="#">156</a>                         |
| Configuring IP Office in normal operation with SCEP disabled<br>.....                            | <a href="#">155</a>                         |
| Configuring IP Office in normal operation with SCEP enabled<br>.....                             | <a href="#">154</a>                         |
| Configuring IP Office when primary is active .....                                               | <a href="#">154</a> , <a href="#">155</a>   |
| configuring IP Office when primary nonfunctional .....                                           | <a href="#">156</a>                         |
| Configuring Linux-based CS1000 servers .....                                                     | <a href="#">140</a>                         |
| Configuring Messaging during GR failback .....                                                   | <a href="#">146</a>                         |
| Configuring Messaging during split network .....                                                 | <a href="#">147</a>                         |
| Configuring Messaging in normal operational mode .....                                           | <a href="#">145</a>                         |
| Configuring Messaging when primary server is<br>nonoperational .....                             | <a href="#">145</a>                         |
| configuring notify sync .....                                                                    | <a href="#">1501</a>                        |
| configuring NTP server .....                                                                     | <a href="#">1530</a>                        |
| configuring Out of Band Management on System Manager<br>.....                                    | <a href="#">1506</a> , <a href="#">1507</a> |
| configuring periodic .....                                                                       | <a href="#">1092</a>                        |
| configuring periodic cleanup .....                                                               | <a href="#">1092</a>                        |
| configuring periodic cleanup for reports .....                                                   | <a href="#">1092</a>                        |
| Configuring Presence Server .....                                                                | <a href="#">144</a>                         |
| configuring Remote Servers .....                                                                 | <a href="#">1093</a>                        |
| Configuring Remote Servers .....                                                                 | <a href="#">1093</a>                        |
| configuring report .....                                                                         | <a href="#">1092</a>                        |
| configuring report properties .....                                                              | <a href="#">1092</a>                        |
| Configuring Session Manager Release 6.2 and earlier during<br>failback .....                     | <a href="#">134</a>                         |
| configuring Session Manager Release 6.2 and earlier during<br>GR failover .....                  | <a href="#">134</a>                         |
| Configuring SIP TLS for CS1000 .....                                                             | <a href="#">1233</a>                        |
| configuring Syslog server .....                                                                  | <a href="#">1529</a>                        |
| configuring System Manager security logs .....                                                   | <a href="#">1529</a>                        |
| configuring time zone .....                                                                      | <a href="#">1530</a>                        |
| configuring trap listener .....                                                                  | <a href="#">889</a>                         |
| configuring trust management .....                                                               | <a href="#">890</a>                         |
| configuring two-way TLS .....                                                                    | <a href="#">1503</a>                        |
| Configuring user settings .....                                                                  | <a href="#">1287</a>                        |
| Configuring VxWorks-based CS1000 servers .....                                                   | <a href="#">140</a>                         |
| confirming identity certificate updates .....                                                    | <a href="#">1232</a>                        |
| Connection Pooling .....                                                                         | <a href="#">985</a>                         |
| configure .....                                                                                  | <a href="#">985</a>                         |
| create .....                                                                                     | <a href="#">985</a>                         |
| edit .....                                                                                       | <a href="#">985</a>                         |
| field descriptions .....                                                                         | <a href="#">987</a>                         |
| connectivity status of the local WebLM servers .....                                             | <a href="#">1051</a>                        |
| console                                                                                          |                                             |
| Tenant Management .....                                                                          | <a href="#">57</a>                          |
| contact                                                                                          |                                             |
| add in default contact list .....                                                                | <a href="#">274</a>                         |
| modify .....                                                                                     | <a href="#">275</a>                         |
| Contact Center                                                                                   |                                             |
| reconfiguring .....                                                                              | <a href="#">157</a>                         |
| contact list member                                                                              |                                             |
| edit .....                                                                                       | <a href="#">278</a>                         |
| contacts                                                                                         |                                             |
| attach .....                                                                                     | <a href="#">276</a>                         |
| content                                                                                          |                                             |
| publishing PDF output .....                                                                      | <a href="#">1535</a>                        |
| searching .....                                                                                  | <a href="#">1535</a>                        |
| sharing .....                                                                                    | <a href="#">1535</a>                        |
| sort by last updated .....                                                                       | <a href="#">1535</a>                        |
| watching for updates .....                                                                       | <a href="#">1535</a>                        |
| Continue on Error .....                                                                          | <a href="#">738</a>                         |
| convert                                                                                          |                                             |
| to stand-alone .....                                                                             | <a href="#">119</a>                         |
| convert .CADF xml file to MIB and trapd .....                                                    | <a href="#">956</a>                         |
| converting .CADF xml file to MIB and trapd .....                                                 | <a href="#">955</a>                         |
| converting .wav audio files .....                                                                | <a href="#">1148</a>                        |
| converting .wav to .c11 audio file format .....                                                  | <a href="#">1148</a>                        |
| converting primary System Manager server to a standalone<br>server .....                         | <a href="#">1220</a>                        |
| converting to .c11 audio files .....                                                             | <a href="#">1148</a>                        |
| cookie domain value                                                                              |                                             |
| SSO .....                                                                                        | <a href="#">1509</a>                        |
| copy                                                                                             |                                             |
| permission .....                                                                                 | <a href="#">197</a>                         |
| Copy All From .....                                                                              | <a href="#">197</a>                         |
| Copy from Role .....                                                                             | <a href="#">197</a>                         |
| copy group .....                                                                                 | <a href="#">161</a>                         |
| copying                                                                                          |                                             |
| CRL .....                                                                                        | <a href="#">106</a>                         |
| copying CM Agent template .....                                                                  | <a href="#">1117</a>                        |
| copying CM Endpoint templates .....                                                              | <a href="#">1120</a>                        |
| copying permission mapping for a role .....                                                      | <a href="#">193</a>                         |
| COR .....                                                                                        | <a href="#">737</a>                         |
| Cord Length .....                                                                                | <a href="#">755</a>                         |
| corporate logo                                                                                   |                                             |
| add .....                                                                                        | <a href="#">74</a>                          |
| Corporate logo .....                                                                             | <a href="#">46</a>                          |
| Corporate Logo .....                                                                             | <a href="#">74</a>                          |
| correcting ESXi host certificate .....                                                           | <a href="#">1349</a>                        |

|                                                                    |            |                                                               |          |
|--------------------------------------------------------------------|------------|---------------------------------------------------------------|----------|
| correlation .....                                                  | 836        | creating a new root CA ( <i>continued</i> ) .....             |          |
| COS .....                                                          | 639        | using option 1 .....                                          | 1217     |
| Station .....                                                      | 737        | creating a new root CA and making it the default CA .....     |          |
| courses .....                                                      | 1536       | command All .....                                             | 1221     |
| Coverage After Forwarding .....                                    | 741        | using option 3 .....                                          | 1221     |
| Coverage Msg Retrieval .....                                       | 750        | creating an SNMP target profile .....                         | 960      |
| Coverage Path .....                                                | 701        | creating an SNMPv3 user profile .....                         | 956      |
| coverage path,                                                     |            | creating a role in vCenter .....                              | 1377     |
| coverage; coverage path .....                                      | 697        | creating basic reports .....                                  | 1085     |
| coverage path, exporting .....                                     | 699        | Creating certificate using certificate signing request .....  | 1214     |
| Coverage Path 1 or Coverage Path 2 .....                           | 738        | creating data backup on remote server .....                   | 843      |
| coverage path list                                                 |            | creating detailed reports .....                               | 1084     |
| coverage; coverage path list .....                                 | 697        | creating discovery profiles .....                             | 899      |
| Coverage Path Number .....                                         | 701        | creating duplicate groups .....                               | 161      |
| coverage time-of-day,                                              |            | creating duplicate user provisioning rule .....               | 617      |
| coverage; coverage time-of-day .....                               | 706        | creating duplicate users .....                                | 231      |
| coverage time-of-day list .....                                    | 706        | creating groups .....                                         | 160      |
| create                                                             |            | creating log harvesting profile .....                         | 1004     |
| new user profile .....                                             | 225        | creating new instance .....                                   | 898      |
| profiles .....                                                     | 899        | creating new user account .....                               | 225      |
| site .....                                                         | 1256       | creating notification filter profile .....                    | 963      |
| team .....                                                         | 1256       | Creating NRP .....                                            | 834, 835 |
| tenant .....                                                       | 1256       | Creating NRP groups .....                                     | 834, 835 |
| tenant organization .....                                          | 1256       | creating SCS profiles .....                                   | 912      |
| user account .....                                                 | 225        | creating software library .....                               | 1303     |
| virtual machine .....                                              | 1352       | creating SRS profiles .....                                   | 912      |
| createCA .....                                                     | 1216       | creating system data backup on a local server .....           | 842      |
| create certificate signing request .....                           | 1212       | creating use profile .....                                    | 637, 639 |
| Create Discovery Profile                                           |            | creating user profile using user provisioning rule .....      | 226      |
| field descriptions .....                                           | 902        | creating user provisioning rule .....                         | 616      |
| create discovery profiles .....                                    | 899        | creating user synchronization job .....                       | 91       |
| create duplicate groups .....                                      | 161        | creation                                                      |          |
| create filter profiles .....                                       | 966        | new CRL .....                                                 | 1233     |
| create new Certificate Authority with SHA256withRSA and 2048 ..... | 1216       | Criteria for migrating 96x1 SIP set type to J1xx set type ... | 725      |
| create new Certificate Authority with SHA2 and 2048 .....          | 1216       | CRL                                                           |          |
| Create New Profile if it doesn't exist for the user .....          | 234        | configuring download .....                                    | 1234     |
| create synchronization job .....                                   | 91         | configuring download job .....                                | 1234     |
| Create Tenant page .....                                           | 1267       | creating new .....                                            | 1233     |
| create user                                                        |            | deleting download job .....                                   | 1236     |
| user provisioning rule .....                                       | 226, 227   | download .....                                                | 1234     |
| create using user provisioning rule                                |            | scheduling download .....                                     | 1234     |
| user profile .....                                                 | 226        | scheduling download job .....                                 | 1234     |
| creating                                                           |            | viewing download job .....                                    | 1236     |
| browser certificate .....                                          | 55         | CRL download                                                  |          |
| duplicate user provisioning rule .....                             | 617        | configuring .....                                             | 1234     |
| generic CSR .....                                                  | 1211, 1341 | scheduling .....                                              | 1234     |
| new CRL .....                                                      | 1233       | CRL download configuration                                    |          |
| user provisioning rule .....                                       | 616        | field descriptions .....                                      | 1236     |
| creating a browser certificate .....                               | 55         | CRL download configuration field descriptions .....           | 1236     |
| creating access profile .....                                      | 920        | CRL download job                                              |          |
| Creating a Certificate Signing Request .....                       | 1212       | deleting .....                                                | 1236     |
| creating an end entity .....                                       | 1213       | viewing .....                                                 | 1236     |
| creating a new communication address for a profile .....           | 259        | CRL download job details                                      |          |
| creating a new port .....                                          | 921        | field descriptions .....                                      | 1237     |
| creating a new root CA                                             |            | CRL download job details field descriptions .....             | 1237     |
| command CreateNewCA .....                                          | 1217       | CS 1000                                                       |          |
|                                                                    |            | functionality limitations .....                               | 142      |

|                                               |                      |                                                      |                                             |
|-----------------------------------------------|----------------------|------------------------------------------------------|---------------------------------------------|
| CS 1000 account operations .....              | <a href="#">985</a>  | data modules field descriptions .....                | <a href="#">806</a>                         |
| CS 1000 alarms .....                          |                      | data modules; field descriptions .....               | <a href="#">806</a>                         |
| configure .....                               | <a href="#">139</a>  | data replication .....                               | <a href="#">1070</a> , <a href="#">1071</a> |
| CS 1000 configuration .....                   | <a href="#">139</a>  | data replication service .....                       | <a href="#">1070</a>                        |
| CS1000 Presence users .....                   | <a href="#">271</a>  | Data Restriction .....                               | <a href="#">750</a>                         |
| CS 1000 profile administration .....          | <a href="#">269</a>  | data retention .....                                 |                                             |
| CS1000 server .....                           |                      | applying data retention rule .....                   | <a href="#">861</a>                         |
| configuration .....                           | <a href="#">140</a>  | editing data retention rule .....                    | <a href="#">861</a>                         |
| CSR .....                                     |                      | field descriptions .....                             | <a href="#">862</a>                         |
| create .....                                  | <a href="#">1212</a> | modifying data retention rule .....                  | <a href="#">861</a>                         |
| create field description .....                | <a href="#">1342</a> | data retention rules .....                           | <a href="#">859</a>                         |
| edit field description .....                  | <a href="#">1342</a> | excluded log files from log purging .....            | <a href="#">859</a>                         |
| CSR create .....                              | <a href="#">1212</a> | Data Transport Config field descriptions .....       | <a href="#">872</a>                         |
| Customized .....                              |                      | Data Transport Static Config page .....              | <a href="#">874</a>                         |
| interface .....                               | <a href="#">74</a>   | date and time configuration; verify .....            | <a href="#">1529</a>                        |
| logo .....                                    | <a href="#">74</a>   | deactivate .....                                     |                                             |
| Customized interface .....                    | <a href="#">74</a>   | secondary server .....                               | <a href="#">114</a>                         |
| Customized Interface field descriptions ..... | <a href="#">74</a>   | Default ACL .....                                    | <a href="#">608</a>                         |
| customizing .....                             | <a href="#">1089</a> | default contact .....                                |                                             |
| customizing reports .....                     | <a href="#">1089</a> | add contact list .....                               | <a href="#">274</a>                         |
| custom patch .....                            |                      | default end entities .....                           |                                             |
| upload .....                                  | <a href="#">1413</a> | use new CA .....                                     | <a href="#">1230</a>                        |
| custom reports .....                          | <a href="#">1082</a> | Default Policy rule .....                            | <a href="#">608</a>                         |
| custom role .....                             |                      | default templates .....                              | <a href="#">1114</a>                        |
| add .....                                     | <a href="#">187</a>  | delete .....                                         |                                             |
| delete .....                                  | <a href="#">194</a>  | element .....                                        | <a href="#">943</a>                         |
| edit .....                                    | <a href="#">194</a>  | global user settings import job on first error ..... | <a href="#">407</a>                         |
| custom roles .....                            | <a href="#">186</a>  | hunt group .....                                     | <a href="#">781</a>                         |
| Custom roles .....                            | <a href="#">181</a>  | role .....                                           | <a href="#">194</a>                         |
| custom templates .....                        | <a href="#">1114</a> | subscribers .....                                    | <a href="#">641</a>                         |
| custom tenant administrator role .....        |                      | subscriber templates .....                           | <a href="#">1123</a>                        |
| add .....                                     | <a href="#">189</a>  | tenant .....                                         | <a href="#">1261</a>                        |
| Cvg Enabled for VDN Route-To Party .....      | <a href="#">702</a>  | trunk group .....                                    | <a href="#">786</a>                         |
| CVG Path .....                                | <a href="#">708</a>  | unused port .....                                    | <a href="#">1327</a>                        |
| <b>D</b> .....                                |                      | delete a global user settings import Job .....       | <a href="#">407</a>                         |
| dashboard .....                               |                      | delete alarms .....                                  | <a href="#">992</a>                         |
| login .....                                   | <a href="#">49</a>   | Delete ALL .....                                     | <a href="#">992</a>                         |
| Dashboard .....                               |                      | delete a user import job .....                       | <a href="#">399</a>                         |
| System Manager .....                          | <a href="#">46</a>   | Delete Confirmation Page .....                       | <a href="#">1112</a>                        |
| data backup .....                             |                      | delete contact addresses of a public contact .....   | <a href="#">597</a>                         |
| remote server .....                           | <a href="#">843</a>  | delete custom role .....                             | <a href="#">194</a>                         |
| data backup; schedule .....                   | <a href="#">844</a>  | Deleted Trusted Certificate Confirmation page .....  | <a href="#">1188</a>                        |
| data backup from local server .....           | <a href="#">847</a>  | deleted user .....                                   |                                             |
| database replication .....                    | <a href="#">100</a>  | restoring .....                                      | <a href="#">253</a>                         |
| Database size .....                           | <a href="#">850</a>  | Deleted Users page .....                             | <a href="#">367</a>                         |
| data encryption .....                         | <a href="#">1491</a> | delete element .....                                 | <a href="#">917</a>                         |
| overview .....                                | <a href="#">1489</a> | delete element access profile .....                  | <a href="#">910</a>                         |
| password policy .....                         | <a href="#">1490</a> | Delete Element Confirmation page .....               | <a href="#">943</a>                         |
| remote key server .....                       | <a href="#">1490</a> | delete element instance mapping .....                | <a href="#">1043</a>                        |
| Data entry warning in Excel .....             | <a href="#">376</a>  | delete element instances .....                       | <a href="#">1043</a>                        |
| Data entry warning in Microsoft Excel .....   | <a href="#">376</a>  | delete filter profiles .....                         | <a href="#">966</a>                         |
| Data link error in Excel .....                | <a href="#">375</a>  | Delete Group Confirmation page .....                 | <a href="#">173</a>                         |
| Data link error in Microsoft Excel .....      | <a href="#">375</a>  | delete IP Office endpoint profile of a user .....    | <a href="#">273</a>                         |
| data module list .....                        | <a href="#">804</a>  | Delete IP Office field description .....             | <a href="#">954</a>                         |
| Data Modules .....                            | <a href="#">804</a>  | Delete local WebLM page .....                        | <a href="#">1061</a>                        |
|                                               |                      | delete Local WebLM server .....                      | <a href="#">1061</a>                        |
|                                               |                      | delete mapping .....                                 | <a href="#">1043</a>                        |



|                                                            |                      |                                                         |                      |
|------------------------------------------------------------|----------------------|---------------------------------------------------------|----------------------|
| delete postal addresses of a public contact .....          | <a href="#">596</a>  | deleting coverage time-of-day                           |                      |
| delete public contact of a user .....                      | <a href="#">594</a>  | coverage time-of-day; delete .....                      | <a href="#">707</a>  |
| Delete Selected .....                                      | <a href="#">992</a>  | deleting data modules                                   |                      |
| delete SNMP Access profile .....                           | <a href="#">905</a>  | data modules; delete .....                              | <a href="#">806</a>  |
| delete SNMPv3 user profiles .....                          | <a href="#">957</a>  | deleting element instances .....                        | <a href="#">1043</a> |
| delete users in bulk .....                                 | <a href="#">234</a>  | deleting endpoints                                      |                      |
| deleting                                                   |                      | removing endpoints .....                                | <a href="#">715</a>  |
| application .....                                          | <a href="#">1359</a> | deleting entity class .....                             | <a href="#">1201</a> |
| communication profile .....                                | <a href="#">258</a>  | deleting files from software library .....              | <a href="#">1309</a> |
| CRL download job .....                                     | <a href="#">1236</a> | deleting groups .....                                   | <a href="#">162</a>  |
| endpoint migration job .....                               | <a href="#">733</a>  | deleting hunt group .....                               | <a href="#">781</a>  |
| expired certificates .....                                 | <a href="#">1238</a> | deleting instances .....                                | <a href="#">1043</a> |
| location .....                                             | <a href="#">1318</a> | deleting IP Office endpoint templates .....             | <a href="#">1142</a> |
| metering collector configuration .....                     | <a href="#">1069</a> | deleting IP Office system configuration templates ..... | <a href="#">1146</a> |
| subject names for the entity class .....                   | <a href="#">1208</a> | deleting jobs .....                                     | <a href="#">1100</a> |
| syslog servers .....                                       | <a href="#">1385</a> | deleting notification filter profile .....              | <a href="#">964</a>  |
| upgrade jobs .....                                         | <a href="#">1437</a> | deleting pending jobs .....                             | <a href="#">1100</a> |
| user provisioning rule .....                               | <a href="#">618</a>  | deleting postal addresses of a private contact .....    | <a href="#">283</a>  |
| Deleting                                                   |                      | deleting private contact of a user .....                | <a href="#">282</a>  |
| administrative user .....                                  | <a href="#">77</a>   | deleting reports .....                                  | <a href="#">1092</a> |
| deleting access profile .....                              | <a href="#">921</a>  | deleting scheduled backup job .....                     | <a href="#">846</a>  |
| deleting a communication address .....                     | <a href="#">260</a>  | deleting SNMP Access profile .....                      | <a href="#">905</a>  |
| deleting a communication profile .....                     | <a href="#">258</a>  | deleting SNMP target profiles .....                     | <a href="#">961</a>  |
| deleting agent                                             |                      | deleting software library .....                         | <a href="#">1304</a> |
| agents; delete .....                                       | <a href="#">659</a>  | deleting subnetworks .....                              | <a href="#">909</a>  |
| deleting agents in bulk .....                              | <a href="#">661</a>  | deleting subscriber templates .....                     | <a href="#">1123</a> |
| deleting a location .....                                  | <a href="#">1318</a> | deleting synchronization datasource, .....              | <a href="#">85</a>   |
| deleting an address .....                                  | <a href="#">255</a>  | deleting templates                                      |                      |
| deleting an announcement .....                             | <a href="#">673</a>  | subscriber .....                                        | <a href="#">1123</a> |
| deleting an audio file in IP Office system configuration   |                      | deleting trunk group .....                              | <a href="#">786</a>  |
| template .....                                             | <a href="#">1149</a> | deleting udp group .....                                | <a href="#">825</a>  |
| deleting an audio group .....                              | <a href="#">684</a>  | deleting uniform dial plan group .....                  | <a href="#">825</a>  |
| deleting an CM Endpoint profile .....                      | <a href="#">265</a>  | deleting user provisioning rule .....                   | <a href="#">618</a>  |
| deleting an element access profile .....                   | <a href="#">910</a>  | deleting user synchronization jobs .....                | <a href="#">93</a>   |
| deleting an element instance .....                         | <a href="#">1043</a> | deleting vCenter .....                                  | <a href="#">1380</a> |
| deleting announcements .....                               | <a href="#">673</a>  | deleting vector directory number                        |                      |
| deleting anonymous profiles .....                          | <a href="#">982</a>  | vector directory number; delete .....                   | <a href="#">690</a>  |
| deleting an SNMP target profile .....                      | <a href="#">961</a>  | deleting vector routing tables                          |                      |
| deleting an SNMPv3 user profile .....                      | <a href="#">957</a>  | vector routing table; delete .....                      | <a href="#">694</a>  |
| deleting a port .....                                      | <a href="#">922</a>  | department                                              |                      |
| deleting a profile .....                                   | <a href="#">1007</a> | create .....                                            | <a href="#">1256</a> |
| Deleting a Remote Server .....                             | <a href="#">1094</a> | editing .....                                           | <a href="#">1261</a> |
| deleting a shared address .....                            | <a href="#">605</a>  | viewing .....                                           | <a href="#">1260</a> |
| deleting a station profile .....                           | <a href="#">268</a>  | deploy                                                  |                      |
| Deleting a UCM and Application Server System Configuration |                      | Branch Session Manager .....                            | <a href="#">1352</a> |
| template .....                                             | <a href="#">1152</a> | Communication Manager .....                             | <a href="#">1352</a> |
| deleting audio groups .....                                | <a href="#">684</a>  | Session Manager .....                                   | <a href="#">1352</a> |
| Deleting a VMPro Call Flow template .....                  | <a href="#">1159</a> | System Manager .....                                    | <a href="#">1352</a> |
| Deleting a VMPro System Configuration template .....       | <a href="#">1156</a> | Utility Services .....                                  | <a href="#">1352</a> |
| deleting bulk user edit jobs .....                         | <a href="#">234</a>  | deploy application .....                                | <a href="#">1316</a> |
| deleting CM Agent template .....                           | <a href="#">1117</a> | deploy Avaya Aura application .....                     | <a href="#">1352</a> |
| deleting CM Endpoint templates .....                       | <a href="#">1119</a> | deploying                                               |                      |
| deleting completed jobs .....                              | <a href="#">1100</a> | AVP Utilities .....                                     | <a href="#">1351</a> |
| deleting contact addresses of a private contact .....      | <a href="#">286</a>  | deploy OVA .....                                        | <a href="#">1352</a> |
| deleting contacts from the contact list .....              | <a href="#">276</a>  | Desktop Video Conferencing .....                        | <a href="#">744</a>  |
| deleting coverage path                                     |                      | determine System Manager that manages GR-aware element  |                      |
| coverage path; delete .....                                | <a href="#">699</a>  |                                                         | <a href="#">916</a>  |

## Index

|                                                            |      |                                                         |            |
|------------------------------------------------------------|------|---------------------------------------------------------|------------|
| device list .....                                          | 901  | displaying ( <i>continued</i> )                         |            |
| Direct IP-IP Audio Connections                             |      | subject names for an entity class .....                 | 1207       |
| Attendant Console .....                                    | 750  | Displaying the password policies .....                  | 69         |
| directory synchronization .....                            | 80   | Display Language .....                                  | 742        |
| Disable Confirmation page .....                            | 1110 | distributing new root CA with Communication Manager ..  | 1219       |
| disable self provisioning .....                            | 221  | distributing the new root CA with 96x1 series phones .. | 1219       |
| disabling                                                  |      | DND/SAC/Go to Cover                                     |            |
| completed jobs .....                                       | 1101 | All .....                                               | 703        |
| Geo Redundancy replication .....                           | 112  | Coverage Path .....                                     | 703        |
| local key store .....                                      | 1495 | Don't Answer .....                                      | 703        |
| outbound connection logging .....                          | 1171 | documentation                                           |            |
| outbound firewall rule .....                               | 1175 | System Manager .....                                    | 1533       |
| pending jobs .....                                         | 1101 | documentation center .....                              | 1535       |
| SSH on Appliance Virtualization Platform .....             | 1331 | finding content .....                                   | 1535       |
| Disabling                                                  |      | navigation .....                                        | 1535       |
| administrative user .....                                  | 77   | documentation portal .....                              | 1535       |
| disabling centralized licensing .....                      | 1044 | finding content .....                                   | 1535       |
| disabling security hardening .....                         | 1167 | navigation .....                                        | 1535       |
| disabling SSH .....                                        | 1332 | domain control .....                                    | 778        |
| disabling the Geographic Redundancy replication for System |      | domain control SIP endpoints                            |            |
| Manager .....                                              | 1220 | enable reachability .....                               | 778        |
| disabling the outbound firewall rule .....                 | 1175 | download                                                |            |
| disaster recovery .....                                    | 129  | harvested log files .....                               | 1009       |
| disaster recovery on primary server                        |      | downloading                                             |            |
| add trusted certificate .....                              | 125  | software .....                                          | 1445       |
| configure CRL download .....                               | 124  | System Manager PEM certificate .....                    | 153, 1498  |
| disaster recovery primary server                           |      | downloading an announcement .....                       | 674        |
| prerequisites .....                                        | 124  | downloading announcements .....                         | 674        |
| discover                                                   |      | downloading audio groups .....                          | 684        |
| device .....                                               | 901  | downloading bulk import spreadsheet .....               | 1421       |
| discover 96x1 SIP set type .....                           | 726  | downloading excel template                              |            |
| discover elements .....                                    | 899  | coverage paths .....                                    | 701        |
| discovering elements .....                                 | 899  | download excel template .....                           | 692        |
| discovering endpoints for migration .....                  | 727  | download excel template hunt groups .....               | 783        |
| discovering SCS servers .....                              | 912  | Downloading Excel template .....                        | 381        |
| discovering SRS servers .....                              | 912  | downloading excel template endpoints .....              | 725        |
| Discover Now .....                                         | 901  | downloading harvested log files .....                   | 1009       |
| Discover SCS server                                        |      | downloading new root CA .....                           | 1218       |
| field descriptions .....                                   | 914  | downloading reports .....                               | 1090       |
| discover SCS servers .....                                 | 911  | downloading the .pem file .....                         | 1499       |
| Discover SRS server                                        |      | downloading the .pem file to Communication Manager ...  | 1499       |
| field descriptions .....                                   | 914  | downloading upgrade files .....                         | 1483       |
| discover SRS servers .....                                 | 911  | download manager                                        |            |
| discovery                                                  |      | downloading software releases .....                     | 1483       |
| profiles .....                                             | 899  | uploading custom patch .....                            | 1413       |
| Discovery Job Status .....                                 | 901  | download software .....                                 | 1307, 1312 |
| discovery profiles                                         |      | DRS .....                                               | 1070, 1071 |
| create .....                                               | 899  | DRS client audit .....                                  | 1071       |
| Discovery Profiles .....                                   | 901  | DRS clients .....                                       | 1071       |
| field descriptions .....                                   | 901  | duplicate                                               |            |
| disk space for                                             |      | subscriber templates .....                              | 1123       |
| System Manager backup .....                                | 840  | Duplicate Group page .....                              | 174        |
| display .....                                              | 1192 | duplicate groups; create .....                          | 161        |
| Display Client Redirection .....                           | 750  | duplicate user provisioning rule                        |            |
| displaying                                                 |      | creating .....                                          | 617        |
| password policies .....                                    | 69   | Duplicate User Provisioning Rule                        |            |
| slots assignment and remote key server .....               | 1494 | field descriptions .....                                | 619        |



|                                                         |                                             |                                                                   |                                            |
|---------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------|--------------------------------------------|
| duplicating an endpoint .....                           | <a href="#">714</a>                         | editing ( <i>continued</i> )                                      |                                            |
| Duplicating a VMPro call flow template .....            | <a href="#">1161</a>                        | team .....                                                        | <a href="#">1261</a>                       |
| Duplicating a VMPro System Configuration template ..... | <a href="#">1157</a>                        | tenant .....                                                      | <a href="#">1261</a>                       |
| duplicating CM Agent template .....                     | <a href="#">1117</a>                        | trunk group .....                                                 | <a href="#">785</a>                        |
| duplicating CM Endpoint templates .....                 | <a href="#">1120</a>                        | vCenter .....                                                     | <a href="#">1380</a>                       |
| duplicating IP Office endpoint templates .....          | <a href="#">1142</a>                        | Editing                                                           |                                            |
| duplicating subscriber templates .....                  | <a href="#">1123</a>                        | administrative user details .....                                 | <a href="#">76</a>                         |
| duplicating templates                                   |                                             | administrative user roles .....                                   | <a href="#">76</a>                         |
| subscribers .....                                       | <a href="#">1123</a>                        | completed jobs .....                                              | <a href="#">845</a>                        |
| duration                                                |                                             | pending jobs .....                                                | <a href="#">845</a> , <a href="#">1100</a> |
| backup and restore .....                                | <a href="#">851</a>                         | editing, user address .....                                       | <a href="#">254</a>                        |
| CS 1000 account operations .....                        | <a href="#">985</a>                         | editing a coverage path                                           |                                            |
| DVC .....                                               | <a href="#">744</a>                         | coverage path; edit .....                                         | <a href="#">698</a>                        |
| <b>E</b>                                                |                                             | editing agent data                                                |                                            |
| EASG login overview                                     |                                             | agents; edit data .....                                           | <a href="#">659</a>                        |
| System Manager .....                                    | <a href="#">1560</a>                        | editing an announcement .....                                     | <a href="#">672</a>                        |
| edit                                                    |                                             | editing an audio group .....                                      | <a href="#">683</a>                        |
| application .....                                       | <a href="#">1358</a>                        | editing an element access profile .....                           | <a href="#">910</a>                        |
| communication profile password policy .....             | <a href="#">610</a>                         | editing an IP Office endpoint profile .....                       | <a href="#">272</a>                        |
| custom role .....                                       | <a href="#">194</a>                         | editing announcements .....                                       | <a href="#">672</a>                        |
| grace period .....                                      | <a href="#">880</a>                         | editing an SNMP target profile .....                              | <a href="#">961</a>                        |
| hunt group .....                                        | <a href="#">781</a>                         | editing an SNMPv3 user profile .....                              | <a href="#">957</a>                        |
| scheduled job .....                                     | <a href="#">1108</a>                        | editing a platform .....                                          | <a href="#">1321</a>                       |
| site .....                                              | <a href="#">1261</a>                        | Editing a Remote Server details .....                             | <a href="#">1094</a>                       |
| subscriber templates .....                              | <a href="#">1122</a>                        | editing a trunk group .....                                       | <a href="#">785</a>                        |
| Edit Address page .....                                 | <a href="#">291</a> , <a href="#">606</a>   | Editing a UCM and Application Server Configuration template ..... | <a href="#">1151</a>                       |
| edit agent data in bulk,                                |                                             | editing audio groups .....                                        | <a href="#">683</a>                        |
| agents; bulk edit .....                                 | <a href="#">660</a>                         | editing authorization code                                        |                                            |
| Edit Appender page .....                                | <a href="#">1021</a>                        | authorization code; edit .....                                    | <a href="#">818</a>                        |
| edit application .....                                  | <a href="#">1358</a>                        | Editing Automatic Alternate Routing Digit Conversion data         |                                            |
| edit assignment of a license file .....                 | <a href="#">1042</a>                        | Automatic Alternate Routing Digit Conversion; editing             |                                            |
| edit authentication scheme .....                        | <a href="#">1240</a>                        | data .....                                                        | <a href="#">796</a>                        |
| Edit Common Console Profile page .....                  | <a href="#">879</a>                         | editing automatic route selection digit conversion data           |                                            |
| edit Communication Profile Password Policy              |                                             | automatic route selection digit conversion; edit data ..          | <a href="#">799</a>                        |
| field descriptions .....                                | <a href="#">611</a>                         | editing automatic route selection toll data                       |                                            |
| edit contact in a contact list .....                    | <a href="#">275</a>                         | automatic route selection toll; edit data .....                   | <a href="#">801</a>                        |
| edit contact list member page .....                     | <a href="#">278</a>                         | Editing a VMPro call flow template .....                          | <a href="#">1159</a>                       |
| Edit Discovery Profile                                  |                                             | Editing a VMPro System Configuration template .....               | <a href="#">1155</a>                       |
| field descriptions .....                                | <a href="#">902</a>                         | editing class of service data .....                               | <a href="#">814</a>                        |
| edit element access profile .....                       | <a href="#">910</a>                         | editing class of service group                                    |                                            |
| edit element instances .....                            | <a href="#">1043</a>                        | class of service group; edit .....                                | <a href="#">820</a>                        |
| Edit Element page .....                                 | <a href="#">936</a>                         | editing CM Agent template .....                                   | <a href="#">1116</a>                       |
| edit endpoint                                           |                                             | editing CM Endpoint templates .....                               | <a href="#">1118</a>                       |
| field descriptions .....                                | <a href="#">735</a>                         | editing coverage time-of-day                                      |                                            |
| edit endpoint extension                                 |                                             | coverage time-of-day; edit .....                                  | <a href="#">707</a>                        |
| field descriptions .....                                | <a href="#">769</a>                         | editing data modules                                              |                                            |
| edit endpoint templates                                 |                                             | data modules; edit .....                                          | <a href="#">805</a>                        |
| field descriptions .....                                | <a href="#">735</a>                         | editing element instances .....                                   | <a href="#">1042</a>                       |
| edit filter profiles .....                              | <a href="#">966</a>                         | editing entity class .....                                        | <a href="#">1201</a>                       |
| Edit Group page .....                                   | <a href="#">172</a>                         | editing hunt group .....                                          | <a href="#">781</a>                        |
| editing                                                 |                                             | editing inactive account deactivation policy                      |                                            |
| clusters .....                                          | <a href="#">803</a>                         | field descriptions .....                                          | <a href="#">72</a>                         |
| department .....                                        | <a href="#">1261</a>                        | editing IP Office endpoint templates .....                        | <a href="#">1141</a>                       |
| generic CSR .....                                       | <a href="#">1211</a> , <a href="#">1341</a> | editing IP Office system configuration templates .....            | <a href="#">1145</a>                       |
| location .....                                          | <a href="#">1317</a>                        | editing log harvesting profile .....                              | <a href="#">1005</a>                       |
|                                                         |                                             | editing notification filter profile .....                         | <a href="#">964</a>                        |

|                                                           |                      |                                                     |                                             |
|-----------------------------------------------------------|----------------------|-----------------------------------------------------|---------------------------------------------|
| Editing Off PBX Configuration Set .....                   | <a href="#">787</a>  | Edit Profile System Manager page .....              | <a href="#">874</a>                         |
| Editing Off PBX Endpoint Mapping .....                    | <a href="#">790</a>  | Edit Public Contact List page .....                 | <a href="#">599</a>                         |
| editing password policies .....                           | <a href="#">60</a>   | Edit Scheduler Profile page .....                   | <a href="#">888</a>                         |
| editing Remote Servers .....                              | <a href="#">1094</a> | edit SNMP access profile .....                      | <a href="#">904</a>                         |
| Editing report .....                                      | <a href="#">1088</a> | edit synchronization datasources .....              | <a href="#">84</a>                          |
| Editing report parameters .....                           | <a href="#">1088</a> | Edit Upgrade Configuration                          |                                             |
| editing session properties .....                          | <a href="#">71</a>   | AVP Configuration .....                             | <a href="#">1405</a>                        |
| field descriptions .....                                  | <a href="#">71</a>   | Element Configuration .....                         | <a href="#">1405</a>                        |
| editing SNMP Access profile .....                         | <a href="#">904</a>  | edit user                                           |                                             |
| editing SNMPv3 user profiles .....                        | <a href="#">957</a>  | user provisioning rule .....                        | <a href="#">227</a>                         |
| editing software library .....                            | <a href="#">1304</a> | Edit User Provisioning Rule                         |                                             |
| editing subscriber templates CMM; field description ..... | <a href="#">1135</a> | field descriptions .....                            | <a href="#">619</a>                         |
| editing subscriber templates .....                        | <a href="#">1122</a> | edit users in bulk .....                            | <a href="#">233</a> , <a href="#">235</a>   |
| editing subscriber templates Messaging                    |                      | Edit vCenter .....                                  | <a href="#">1381</a>                        |
| field descriptions .....                                  | <a href="#">1132</a> | EJBCA .....                                         | <a href="#">1178</a> , <a href="#">1224</a> |
| editing subscriber templates MM; field description .....  | <a href="#">1137</a> | EJBCA to Sub CA .....                               | <a href="#">1224</a>                        |
| editing templates                                         |                      | element                                             |                                             |
| subscriber .....                                          | <a href="#">1122</a> | add .....                                           | <a href="#">898</a> , <a href="#">1427</a>  |
| editing tenant .....                                      | <a href="#">1261</a> | create .....                                        | <a href="#">898</a>                         |
| editing the location .....                                | <a href="#">1317</a> | create Communication Manager .....                  | <a href="#">915</a>                         |
| editing the login warning banner .....                    | <a href="#">73</a>   | create Messaging .....                              | <a href="#">915</a>                         |
| editing the properties of an element instance .....       | <a href="#">1042</a> | delete .....                                        | <a href="#">917</a> , <a href="#">943</a>   |
| editing the select all attribute .....                    | <a href="#">650</a>  | edit .....                                          | <a href="#">917</a>                         |
| editing UDP entries .....                                 | <a href="#">828</a>  | import .....                                        | <a href="#">898</a>                         |
| editing UDP Group .....                                   | <a href="#">824</a>  | new .....                                           | <a href="#">898</a>                         |
| editing Uniform Dial Plan Group .....                     | <a href="#">824</a>  | view .....                                          | <a href="#">916</a>                         |
| editing upgrade configuration .....                       | <a href="#">1437</a> | Element                                             |                                             |
| editing vCenter .....                                     | <a href="#">1380</a> | Cut Through .....                                   | <a href="#">779</a>                         |
| editing vector directory number;                          |                      | element access profile                              |                                             |
| vector directory number; edit .....                       | <a href="#">689</a>  | add .....                                           | <a href="#">909</a>                         |
| editing vector routing table .....                        | <a href="#">693</a>  | delete .....                                        | <a href="#">910</a>                         |
| editing xmobile configuration                             |                      | edit .....                                          | <a href="#">910</a>                         |
| xmobile configuration; edit .....                         | <a href="#">792</a>  | Element Access Profile Management .....             | <a href="#">911</a>                         |
| edit IPOffice.properties file .....                       | <a href="#">274</a>  | Element Cut-Through .....                           | <a href="#">652</a> , <a href="#">709</a>   |
| Edit Location .....                                       | <a href="#">1318</a> | Element Cut-Through; access .....                   | <a href="#">709</a>                         |
| edit logger .....                                         | <a href="#">1018</a> | element data export .....                           | <a href="#">918</a>                         |
| Edit Logger page .....                                    | <a href="#">1020</a> | element export from System Manager CLI .....        | <a href="#">917</a>                         |
| edit password policies                                    |                      | element instance                                    |                                             |
| field description .....                                   | <a href="#">61</a>   | delete .....                                        | <a href="#">1043</a>                        |
| Edit Platform .....                                       | <a href="#">1343</a> | edit .....                                          | <a href="#">1042</a>                        |
| Edit Private Contact List page .....                      | <a href="#">288</a>  | edit properties .....                               | <a href="#">1042</a>                        |
| Edit Profile:Alarming UI page .....                       | <a href="#">878</a>  | remove .....                                        | <a href="#">1043</a>                        |
| Edit Profile:Communication System Management              |                      | element instance field description .....            | <a href="#">1043</a>                        |
| Configuration page .....                                  | <a href="#">867</a>  | element management .....                            | <a href="#">896</a>                         |
| Edit Profile: Configuration page                          |                      | Element Manager                                     |                                             |
| Inventory .....                                           | <a href="#">870</a>  | redirect CS 1000 user .....                         | <a href="#">269</a>                         |
| Edit Profile:GracefulShutdown .....                       | <a href="#">880</a>  | elements                                            |                                             |
| Edit Profile:HealthMonitor UI page .....                  | <a href="#">881</a>  | discover .....                                      | <a href="#">899</a>                         |
| Edit Profile: Inventory page .....                        | <a href="#">870</a>  | import .....                                        | <a href="#">944</a>                         |
| Edit Profile:Licenses page .....                          | <a href="#">882</a>  | refresh .....                                       | <a href="#">1311</a> , <a href="#">1355</a> |
| Edit Profile:Logging page .....                           | <a href="#">883</a>  | Elements Geographic Redundancy manageability status |                                             |
| Edit Profile:Logging Service page .....                   | <a href="#">885</a>  | matrix .....                                        | <a href="#">132</a>                         |
| Edit Profile: Trust Management field description .....    | <a href="#">891</a>  | elements upgrade                                    |                                             |
| Edit profile Messaging field descriptions .....           | <a href="#">871</a>  | target release .....                                | <a href="#">1396</a>                        |
| Edit Profile SMGR Element Manager                         |                      | element upgrade .....                               | <a href="#">1402</a>                        |
| field descriptions .....                                  | <a href="#">885</a>  | Emergency Location Ext .....                        | <a href="#">737</a>                         |
| Edit Profile SMGR Element Manager field descriptions .... | <a href="#">885</a>  | EMU Login Allowed .....                             | <a href="#">753</a>                         |

|                                                              |                                           |  |
|--------------------------------------------------------------|-------------------------------------------|--|
| enable                                                       |                                           |  |
| commercial grade hardening .....                             | <a href="#">1163</a>                      |  |
| military grade hardening .....                               | <a href="#">1164</a>                      |  |
| Multi Tenancy .....                                          | <a href="#">874</a>                       |  |
| password strength policy .....                               | <a href="#">60</a>                        |  |
| enable self provisioning .....                               | <a href="#">221</a>                       |  |
| enabling .....                                               | <a href="#">1040</a>                      |  |
| backup encryption .....                                      | <a href="#">842</a>                       |  |
| certificate based authentication .....                       | <a href="#">54</a>                        |  |
| Extended Hostname Validation .....                           | <a href="#">1239</a>                      |  |
| FTP .....                                                    | <a href="#">1293</a>                      |  |
| Geographic Redundancy replication .....                      | <a href="#">111</a>                       |  |
| local key store .....                                        | <a href="#">1495</a>                      |  |
| Multi Tenancy .....                                          | <a href="#">1255</a>                      |  |
| outbound connection logging .....                            | <a href="#">1170</a>                      |  |
| Setup.sh .....                                               | <a href="#">1293</a>                      |  |
| Setup.sh stop .....                                          | <a href="#">1293</a>                      |  |
| SSH on Appliance Virtualization Platform .....               | <a href="#">1331</a>                      |  |
| System Manager .....                                         | <a href="#">1293</a>                      |  |
| Enabling                                                     |                                           |  |
| administrative user .....                                    | <a href="#">77</a>                        |  |
| completed jobs .....                                         | <a href="#">1102</a>                      |  |
| pending jobs .....                                           | <a href="#">1102</a>                      |  |
| enabling backup encryption .....                             | <a href="#">842</a>                       |  |
| enabling CLI access                                          |                                           |  |
| System Manager web console .....                             | <a href="#">56</a>                        |  |
| enabling security hardening                                  |                                           |  |
| security hardening .....                                     | <a href="#">1166</a>                      |  |
| enabling SSH .....                                           | <a href="#">1332</a>                      |  |
| enabling the Discover Endpoint eligible for migration job .. | <a href="#">727</a>                       |  |
| enabling two-way TLS .....                                   | <a href="#">1504</a>                      |  |
| encryptionLocalKey .....                                     | <a href="#">1495</a>                      |  |
| encryptionPassphrase .....                                   | <a href="#">1491</a>                      |  |
| encryptionRemoteKey .....                                    | <a href="#">1493</a>                      |  |
| encrypt passwords .....                                      | <a href="#">394</a> , <a href="#">395</a> |  |
| end entry                                                    |                                           |  |
| create .....                                                 | <a href="#">1213</a>                      |  |
| endpoint                                                     |                                           |  |
| adding dependencies .....                                    | <a href="#">833</a>                       |  |
| administration .....                                         | <a href="#">711</a>                       |  |
| change parameters globally .....                             | <a href="#">718</a>                       |  |
| duplicate .....                                              | <a href="#">714</a>                       |  |
| management .....                                             | <a href="#">711</a>                       |  |
| save as template .....                                       | <a href="#">715</a>                       |  |
| endpoint display mode .....                                  | <a href="#">759</a>                       |  |
| Endpoint editor                                              |                                           |  |
| permissions .....                                            | <a href="#">202</a>                       |  |
| endpoint extension .....                                     | <a href="#">769</a>                       |  |
| edit .....                                                   | <a href="#">716</a>                       |  |
| editing endpoint extension .....                             | <a href="#">716</a>                       |  |
| endpoint list .....                                          | <a href="#">723</a>                       |  |
| Endpoint options .....                                       | <a href="#">831</a>                       |  |
| endpoints .....                                              | <a href="#">711</a>                       |  |
| add .....                                                    | <a href="#">712</a>                       |  |
| assign range .....                                           | <a href="#">209</a>                       |  |
| change set type of endpoints .....                           | <a href="#">773</a>                       |  |
| field-level RBAC .....                                       | <a href="#">211</a>                       |  |
| endpoints ( <i>continued</i> )                               |                                           |  |
| range .....                                                  | <a href="#">208</a> , <a href="#">209</a> |  |
| releasing .....                                              | <a href="#">721</a>                       |  |
| remove dependencies .....                                    | <a href="#">833</a>                       |  |
| swap .....                                                   | <a href="#">770</a>                       |  |
| Endpoints                                                    |                                           |  |
| Element Cut Through .....                                    | <a href="#">779</a>                       |  |
| endpoints, exporting .....                                   | <a href="#">723</a>                       |  |
| endpoints; bulk add                                          |                                           |  |
| bulk add endpoints .....                                     | <a href="#">716</a>                       |  |
| Endpoints; bulk delete .....                                 | <a href="#">717</a>                       |  |
| endpoints; busy out                                          |                                           |  |
| busy out endpoint .....                                      | <a href="#">720</a>                       |  |
| endpoints; delete .....                                      | <a href="#">715</a>                       |  |
| endpoints; edit                                              |                                           |  |
| editing endpoints .....                                      | <a href="#">713</a>                       |  |
| endpoints; status                                            |                                           |  |
| endpoint status .....                                        | <a href="#">720</a>                       |  |
| endpoints; testing                                           |                                           |  |
| testing endpoints .....                                      | <a href="#">721</a>                       |  |
| endpoints; view                                              |                                           |  |
| viewing endpoints .....                                      | <a href="#">714</a>                       |  |
| endpoint template list .....                                 | <a href="#">1124</a>                      |  |
| endpoint template versions .....                             | <a href="#">1114</a>                      |  |
| end user change communication profile password .....         | <a href="#">223</a>                       |  |
| end user self provisioning .....                             | <a href="#">221</a> , <a href="#">223</a> |  |
| Enhanced Call Fwd .....                                      | <a href="#">756</a>                       |  |
| enrollment password .....                                    | <a href="#">1181</a>                      |  |
| generate .....                                               | <a href="#">1181</a>                      |  |
| Enrollment Password page .....                               | <a href="#">1183</a>                      |  |
| ensuring certificate response .....                          | <a href="#">1226</a>                      |  |
| Enterprise Configuration page .....                          | <a href="#">1055</a>                      |  |
| Enterprise Java Beans Certificate Authority .....            | <a href="#">1178</a>                      |  |
| enterprise licensing                                         |                                           |  |
| configure .....                                              | <a href="#">1046</a>                      |  |
| entity class                                                 |                                           |  |
| filter .....                                                 | <a href="#">1201</a>                      |  |
| Equinox Conferencing                                         |                                           |  |
| configuration .....                                          | <a href="#">151</a>                       |  |
| error codes .....                                            | <a href="#">770</a>                       |  |
| error codes for failout results .....                        | <a href="#">770</a>                       |  |
| esxcfg-route .....                                           | <a href="#">1333</a>                      |  |
| esxcli network ip interface ipv4 set -i vmk0 -l .....        | <a href="#">1333</a>                      |  |
| ESXi host                                                    |                                           |  |
| adding .....                                                 | <a href="#">1319</a>                      |  |
| removing .....                                               | <a href="#">1337</a>                      |  |
| restarting .....                                             | <a href="#">1337</a>                      |  |
| ESXi host certificate addition .....                         | <a href="#">1350</a>                      |  |
| ESXi host certificate update .....                           | <a href="#">1349</a>                      |  |
| ESXi host map to unknown location .....                      | <a href="#">1339</a>                      |  |
| Event processor page .....                                   | <a href="#">868</a>                       |  |
| Example                                                      |                                           |  |
| bulk import and export of user by using Excel file .....     | <a href="#">372</a>                       |  |
| Excel                                                        |                                           |  |
| bulk import .....                                            | <a href="#">379</a>                       |  |
| Data entry warning .....                                     | <a href="#">376</a>                       |  |
| Data link error .....                                        | <a href="#">375</a>                       |  |

|                                                            |                                           |                                                                       |
|------------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------------------|
| Excel ( <i>continued</i> )                                 |                                           |                                                                       |
| export                                                     | <a href="#">370</a>                       | external server; system requirements <a href="#">1310</a>             |
| import                                                     | <a href="#">370</a>                       | external server for upgrade <a href="#">1292</a>                      |
| import user                                                | <a href="#">379</a>                       |                                                                       |
| Excel file                                                 |                                           | <b>F</b>                                                              |
| bulk import and export of user                             | <a href="#">372</a>                       | Favorite <a href="#">756</a>                                          |
| import users                                               | <a href="#">580</a>                       | feature options                                                       |
| excel template                                             | <a href="#">692</a> , <a href="#">701</a> | voice mail number <a href="#">753</a>                                 |
| Excel template                                             |                                           | Feature Options <a href="#">740</a>                                   |
| download                                                   | <a href="#">381</a>                       | field description                                                     |
| excel template endpoints                                   | <a href="#">725</a>                       | anonymous communication profiles <a href="#">984</a>                  |
| excel template hunt group                                  | <a href="#">783</a>                       | CM Upgrade Configuration <a href="#">1466</a>                         |
| exchanging CA certificate                                  |                                           | edit elements <a href="#">1428</a>                                    |
| System Manager and Avaya Equinox Management                | <a href="#">152</a>                       | password policies <a href="#">61</a>                                  |
| existing hosts                                             |                                           | SNMP Access Profile <a href="#">906</a>                               |
| managing certificates                                      | <a href="#">1350</a>                      | TrapListener service <a href="#">889</a>                              |
| existing vCenter                                           |                                           | User Settings <a href="#">1291</a>                                    |
| managing certificates                                      | <a href="#">1350</a>                      | field descriptions                                                    |
| export                                                     |                                           | Add Communication Manager <a href="#">947</a>                         |
| communication profile                                      | <a href="#">383</a>                       | Add Entity Class <a href="#">1203</a>                                 |
| contacts                                                   | <a href="#">383</a>                       | Add Mapping <a href="#">196</a>                                       |
| element                                                    | <a href="#">918</a>                       | Add new Administrative Users <a href="#">78</a>                       |
| global user settings                                       | <a href="#">403</a>                       | Add Platform <a href="#">1343</a>                                     |
| user data                                                  | <a href="#">370</a> , <a href="#">376</a> | Add Server <a href="#">1094</a>                                       |
| user data to Excel                                         | <a href="#">370</a>                       | Add Trusted Certificate <a href="#">1185</a>                          |
| export CM Agent profile                                    | <a href="#">370</a>                       | Administrative Users <a href="#">78</a>                               |
| export CM station data                                     | <a href="#">370</a>                       | Agent List <a href="#">970</a>                                        |
| export elements from System Manager CLI                    | <a href="#">917</a>                       | Allocations by Feature <a href="#">1065</a>                           |
| exporting                                                  |                                           | Application Deployment <a href="#">1369</a>                           |
| alarms                                                     | <a href="#">992</a>                       | Applications <a href="#">1386</a>                                     |
| exporting all coverage paths                               | <a href="#">700</a>                       | Application Server System Configuration template <a href="#">1154</a> |
| exporting all endpoints                                    | <a href="#">724</a>                       | ars toll <a href="#">802</a>                                          |
| exporting all hunt groups                                  | <a href="#">782</a>                       | Assigned Users <a href="#">197</a>                                    |
| exporting all vector directory numbers                     | <a href="#">691</a>                       | audit logging configuration <a href="#">1029</a>                      |
| exporting coverage paths                                   | <a href="#">700</a>                       | authentication servers <a href="#">1243</a>                           |
| exporting CS 1000 user data                                | <a href="#">637</a> , <a href="#">639</a> | Auto answer <a href="#">772</a>                                       |
| exporting endpoints                                        | <a href="#">724</a>                       | automatic route selection toll <a href="#">802</a>                    |
| exporting hunt groups                                      | <a href="#">782</a>                       | Change Allocations <a href="#">1066</a>                               |
| exporting selected coverage path                           | <a href="#">699</a>                       | change password <a href="#">1346</a>                                  |
| exporting selected endpoints                               | <a href="#">723</a>                       | Choose Address <a href="#">257</a>                                    |
| exporting selected hunt group                              | <a href="#">782</a>                       | Choose Group <a href="#">180</a>                                      |
| exporting selected hunt group; hunt group                  | <a href="#">782</a>                       | Communication Manager Backup Configuration <a href="#">1466</a>       |
| exporting selected vector directory number                 | <a href="#">690</a>                       | corporate logo <a href="#">74</a>                                     |
| exporting the user data                                    | <a href="#">634</a>                       | Create AVP Kickstart <a href="#">1329</a>                             |
| exporting vector directory number; vector directory number | <a href="#">690</a>                       | create CSR <a href="#">1342</a>                                       |
| exporting vector directory numbers                         | <a href="#">691</a>                       | Create Discovery Profile <a href="#">902</a>                          |
| export logs                                                | <a href="#">1023</a>                      | Create New Profile <a href="#">1012</a>                               |
| exportUpmGlobalsettings command                            | <a href="#">403</a>                       | Create Tenant <a href="#">1267</a>                                    |
| export users                                               | <a href="#">382</a>                       | CRL download configuration <a href="#">1236</a>                       |
| System Manager web console                                 | <a href="#">383</a>                       | CRL download job details <a href="#">1237</a>                         |
| Export Users                                               | <a href="#">386</a>                       | customized interface <a href="#">74</a>                               |
| extended hostname validation                               |                                           | data retention <a href="#">862</a>                                    |
| overview                                                   | <a href="#">1239</a>                      | Data Transport Config <a href="#">872</a>                             |
| Extension                                                  |                                           | Deleted Users page <a href="#">367</a>                                |
| Station                                                    | <a href="#">736</a>                       | Delete Group Confirmation <a href="#">173</a>                         |
| external authentication                                    | <a href="#">1239</a>                      | Discovery Profiles <a href="#">901</a>                                |
|                                                            |                                           | Duplicate User Provisioning Rule <a href="#">619</a>                  |

field descriptions (*continued*)

|                                                 |                      |
|-------------------------------------------------|----------------------|
| edit CSR .....                                  | <a href="#">1342</a> |
| Edit Discovery Profile .....                    | <a href="#">902</a>  |
| edit endpoint extension .....                   | <a href="#">769</a>  |
| Edit Group .....                                | <a href="#">172</a>  |
| Edit Location .....                             | <a href="#">1318</a> |
| Edit Platform .....                             | <a href="#">1343</a> |
| Edit Profile SMGR .....                         | <a href="#">874</a>  |
| Edit Profile SMGR Element Manager .....         | <a href="#">885</a>  |
| Edit Public Contacts .....                      | <a href="#">599</a>  |
| Edit Remote Server .....                        | <a href="#">1094</a> |
| Edit User Provisioning Rule .....               | <a href="#">619</a>  |
| Element Access Profile Management .....         | <a href="#">911</a>  |
| Element Cut-Through .....                       | <a href="#">709</a>  |
| Endpoint Migration .....                        | <a href="#">733</a>  |
| Endpoint Migration Job History .....            | <a href="#">734</a>  |
| Enterprise Usage .....                          | <a href="#">1063</a> |
| Export Users .....                              | <a href="#">386</a>  |
| Filter Profiles .....                           | <a href="#">966</a>  |
| Group Management .....                          | <a href="#">167</a>  |
| Harvest Archives .....                          | <a href="#">1014</a> |
| Host Network / IP Settings .....                | <a href="#">1345</a> |
| Import Global Settings page .....               | <a href="#">584</a>  |
| inactive account deactivation policy .....      | <a href="#">72</a>   |
| IP Office System Configuration template .....   | <a href="#">1147</a> |
| Job History .....                               | <a href="#">1391</a> |
| load AVP host certificate .....                 | <a href="#">1341</a> |
| Locations .....                                 | <a href="#">1386</a> |
| manage certificate revocation .....             | <a href="#">1198</a> |
| Manage Elements .....                           | <a href="#">933</a>  |
| Manage Entity Classes .....                     | <a href="#">1202</a> |
| Manage Trusted Certificates .....               | <a href="#">1189</a> |
| Map vCenter .....                               | <a href="#">1381</a> |
| Metering Collector Configuration .....          | <a href="#">1068</a> |
| Modify Access Profile Entry .....               | <a href="#">911</a>  |
| Move Group .....                                | <a href="#">174</a>  |
| New Group .....                                 | <a href="#">168</a>  |
| New Location .....                              | <a href="#">1318</a> |
| New Public Contact List page .....              | <a href="#">601</a>  |
| New Report .....                                | <a href="#">1085</a> |
| New User Provisioning Rule .....                | <a href="#">619</a>  |
| Notification Filter Profiles .....              | <a href="#">966</a>  |
| Periodic cleanup of reports .....               | <a href="#">869</a>  |
| Platforms .....                                 | <a href="#">1386</a> |
| Preupgrade configuration .....                  | <a href="#">1315</a> |
| provision first LDAP server .....               | <a href="#">1243</a> |
| provision Kerberos server .....                 | <a href="#">1243</a> |
| provision LDAP server .....                     | <a href="#">1243</a> |
| provision RADIUS server .....                   | <a href="#">1243</a> |
| provision SAML remote identity provider .....   | <a href="#">1243</a> |
| provision second LDAP server .....              | <a href="#">1243</a> |
| provision user certificate authentication ..... | <a href="#">1243</a> |
| Remote Server configuration .....               | <a href="#">1094</a> |
| Remote Server Configuration .....               | <a href="#">1095</a> |
| replace identity certificates .....             | <a href="#">1195</a> |
| Replica Nodes .....                             | <a href="#">1076</a> |
| Replication Node Details .....                  | <a href="#">1079</a> |

field descriptions (*continued*)

|                                                                      |                                           |
|----------------------------------------------------------------------|-------------------------------------------|
| Reports Definition List .....                                        | <a href="#">1083</a>                      |
| Reports Generation .....                                             | <a href="#">1083</a>                      |
| Reports History .....                                                | <a href="#">1091</a>                      |
| Resource Synchronization .....                                       | <a href="#">175</a>                       |
| revoke certificate .....                                             | <a href="#">1199</a>                      |
| Roles .....                                                          | <a href="#">194</a>                       |
| schedule CRL download .....                                          | <a href="#">1234</a>                      |
| security configuration .....                                         | <a href="#">1237</a>                      |
| security settings .....                                              | <a href="#">73</a>                        |
| server properties .....                                              | <a href="#">1045</a>                      |
| Serviceability Agents .....                                          | <a href="#">970</a>                       |
| session properties .....                                             | <a href="#">71</a>                        |
| Shutdown System Manager .....                                        | <a href="#">1275</a>                      |
| SNMP Access Profiles .....                                           | <a href="#">905</a>                       |
| Software inventory .....                                             | <a href="#">1460</a>                      |
| Subnet Configurations .....                                          | <a href="#">909</a>                       |
| synchronization job history .....                                    | <a href="#">94</a>                        |
| Synchronize CM Data and Configure Options .....                      | <a href="#">709</a>                       |
| syslog receiver configuration .....                                  | <a href="#">1384</a>                      |
| System Manager Dashboard .....                                       | <a href="#">48</a>                        |
| Tenant Management .....                                              | <a href="#">1267</a>                      |
| UCM and Application Server System Configuration<br>template .....    | <a href="#">1154</a>                      |
| UnAssign Roles .....                                                 | <a href="#">369</a>                       |
| Unified Communications Module System Configuration<br>template ..... | <a href="#">1154</a>                      |
| Update Entity Class .....                                            | <a href="#">1203</a>                      |
| Upgrade Configuration .....                                          | <a href="#">1404</a>                      |
| Upgrade Management .....                                             | <a href="#">1402</a>                      |
| User Bulk Editor .....                                               | <a href="#">235</a>                       |
| User Profile   Add .....                                             | <a href="#">295</a>                       |
| User Profile   Duplicate   <User Name> page .....                    | <a href="#">348</a>                       |
| User Profile   Edit   <User Name> .....                              | <a href="#">315</a>                       |
| User Profile   View   <User Name> page .....                         | <a href="#">333</a>                       |
| User Provisioning Rules .....                                        | <a href="#">235</a> , <a href="#">618</a> |
| User Restore Confirmation Page .....                                 | <a href="#">368</a>                       |
| user synchronization datasource .....                                | <a href="#">85</a>                        |
| user synchronization jobs .....                                      | <a href="#">93</a>                        |
| view by feature .....                                                | <a href="#">1055</a>                      |
| view certificate detail .....                                        | <a href="#">1198</a>                      |
| View Group .....                                                     | <a href="#">170</a>                       |
| Viewing job summary .....                                            | <a href="#">95</a>                        |
| View License Capacity .....                                          | <a href="#">1037</a>                      |
| View Peak Usage .....                                                | <a href="#">1038</a>                      |
| View Profile SMGR .....                                              | <a href="#">874</a>                       |
| View Profile SMGR Element Manager .....                              | <a href="#">885</a>                       |
| View Remote Server .....                                             | <a href="#">1094</a>                      |
| View Trust Certificate .....                                         | <a href="#">1188</a>                      |
| View User Provisioning Rule .....                                    | <a href="#">619</a>                       |
| WebLM Configuration .....                                            | <a href="#">1336</a>                      |
| WebLM Home .....                                                     | <a href="#">1036</a>                      |
| field descriptions, Snapshot Manager .....                           | <a href="#">1343</a>                      |
| field level RBAC .....                                               | <a href="#">204</a>                       |
| Communication Manager objects .....                                  | <a href="#">204</a>                       |
| field-level RBAC in endpoints .....                                  | <a href="#">211</a>                       |
| field-level RBAC in hunt group .....                                 | <a href="#">215</a>                       |

|                                                              |                                           |                                                                                                                                                                                                                                                       |                                                                                       |
|--------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| field-level RBAC in trunk group .....                        | <a href="#">217</a>                       | FTP server                                                                                                                                                                                                                                            |                                                                                       |
| file download manager .....                                  | <a href="#">1313</a>                      | configure as remote .....                                                                                                                                                                                                                             | <a href="#">1296</a>                                                                  |
| file replication .....                                       | <a href="#">100</a>                       | install .....                                                                                                                                                                                                                                         | <a href="#">1296</a>                                                                  |
| file size                                                    |                                           | functions                                                                                                                                                                                                                                             |                                                                                       |
| bulk export user .....                                       | <a href="#">390</a>                       | User Management scheduled job .....                                                                                                                                                                                                                   | <a href="#">1097</a>                                                                  |
| file transfer settings; announcements .....                  | <a href="#">677</a>                       |                                                                                                                                                                                                                                                       |                                                                                       |
| filling                                                      |                                           | <b>G</b>                                                                                                                                                                                                                                              |                                                                                       |
| bulk import spreadsheet .....                                | <a href="#">1422</a>                      | G430 and G450 Media Gateway multistep upgrade .....                                                                                                                                                                                                   | <a href="#">1480</a>                                                                  |
| bulk instances .....                                         | <a href="#">1422</a>                      | G430 Branch Gateway                                                                                                                                                                                                                                   |                                                                                       |
| filter                                                       |                                           | add .....                                                                                                                                                                                                                                             | <a href="#">928</a>                                                                   |
| alarm .....                                                  | <a href="#">962</a>                       | G450 Branch Gateway                                                                                                                                                                                                                                   |                                                                                       |
| informs .....                                                | <a href="#">962</a>                       | add .....                                                                                                                                                                                                                                             | <a href="#">928</a>                                                                   |
| notification .....                                           | <a href="#">962</a>                       | gateway protocol matrix .....                                                                                                                                                                                                                         | <a href="#">1486</a>                                                                  |
| traps .....                                                  | <a href="#">962</a>                       | gateway upgrade                                                                                                                                                                                                                                       |                                                                                       |
| filtering alarms .....                                       | <a href="#">992</a>                       | multistep upgrade .....                                                                                                                                                                                                                               | <a href="#">1480</a>                                                                  |
| filtering announcements .....                                | <a href="#">678</a>                       | General Configuration Details .....                                                                                                                                                                                                                   | <a href="#">1405</a>                                                                  |
| filtering class of service list .....                        | <a href="#">814</a>                       | general guidelines and capabilities                                                                                                                                                                                                                   |                                                                                       |
| filtering Communication Manager objects                      |                                           | user provisioning rules .....                                                                                                                                                                                                                         | <a href="#">614</a>                                                                   |
| using filters; Communication Manager objects .....           | <a href="#">657</a>                       | General Options .....                                                                                                                                                                                                                                 | <a href="#">737</a>                                                                   |
| filtering entity class .....                                 | <a href="#">1201</a>                      | generate                                                                                                                                                                                                                                              |                                                                                       |
| filtering groups .....                                       | <a href="#">165</a>                       | end user communication profile password .....                                                                                                                                                                                                         | <a href="#">222</a>                                                                   |
| filtering jobs .....                                         | <a href="#">1099</a>                      | generate_report.sh .....                                                                                                                                                                                                                              | <a href="#">1375</a>                                                                  |
| filtering log harvesting profiles .....                      | <a href="#">1010</a>                      | generate certificate signing request .....                                                                                                                                                                                                            | <a href="#">1224</a>                                                                  |
| Filtering log harvesting requests .....                      | <a href="#">1010</a>                      | generate communication profile password .....                                                                                                                                                                                                         | <a href="#">222</a>                                                                   |
| filtering logs .....                                         | <a href="#">1023</a>                      | generate identity certificates .....                                                                                                                                                                                                                  | <a href="#">1232</a>                                                                  |
| filtering resources .....                                    | <a href="#">166</a> , <a href="#">177</a> | generate test alarm .....                                                                                                                                                                                                                             | <a href="#">996</a>                                                                   |
| filtering SNMPv3 user profiles .....                         | <a href="#">958</a>                       | generate test alarms .....                                                                                                                                                                                                                            | <a href="#">994</a>                                                                   |
| filtering subscribers                                        |                                           | generateTrapdAndMibUnix .....                                                                                                                                                                                                                         | <a href="#">956</a>                                                                   |
| using filters; subscribers .....                             | <a href="#">642</a>                       | generateTrapdAndMibUnix.sh .....                                                                                                                                                                                                                      | <a href="#">955</a>                                                                   |
| filtering target profiles .....                              | <a href="#">960</a>                       | generating                                                                                                                                                                                                                                            |                                                                                       |
| filtering templates                                          |                                           | certificates .....                                                                                                                                                                                                                                    | <a href="#">1348</a>                                                                  |
| filtering endpoint templates .....                           | <a href="#">1114</a>                      | certificate using CLI .....                                                                                                                                                                                                                           | <a href="#">55</a>                                                                    |
| filtering subscriber templates .....                         | <a href="#">1114</a>                      | endpoint report with buttons .....                                                                                                                                                                                                                    | <a href="#">1082</a>                                                                  |
| using filters; templates .....                               | <a href="#">1114</a>                      | virtual machine report .....                                                                                                                                                                                                                          | <a href="#">1375</a>                                                                  |
| filter profile                                               |                                           | generating basic reports .....                                                                                                                                                                                                                        | <a href="#">1085</a>                                                                  |
| assign to serviceability agent .....                         | <a href="#">964</a>                       | generating certificate                                                                                                                                                                                                                                |                                                                                       |
| create .....                                                 | <a href="#">963</a>                       | for cert-based authentication .....                                                                                                                                                                                                                   | <a href="#">55</a>                                                                    |
| unassign from serviceability agent .....                     | <a href="#">965</a>                       | generating certificate keystore .....                                                                                                                                                                                                                 | <a href="#">1213</a>                                                                  |
| Filter Profiles                                              |                                           | generating detailed reports .....                                                                                                                                                                                                                     | <a href="#">1084</a>                                                                  |
| field descriptions .....                                     | <a href="#">966</a>                       | generating kickstart file                                                                                                                                                                                                                             |                                                                                       |
| filter users .....                                           | <a href="#">247</a>                       | Appliance Virtualization Platform .....                                                                                                                                                                                                               | <a href="#">1328</a>                                                                  |
| finding content on documentation center .....                | <a href="#">1535</a>                      | generating test alarms .....                                                                                                                                                                                                                          | <a href="#">995</a>                                                                   |
| finding port matrix .....                                    | <a href="#">1534</a>                      | generic CSR                                                                                                                                                                                                                                           |                                                                                       |
| firewall basics .....                                        | <a href="#">1539</a>                      | creating .....                                                                                                                                                                                                                                        | <a href="#">1211</a> , <a href="#">1341</a>                                           |
| firewall implementation in System Manager .....              | <a href="#">1539</a>                      | editing .....                                                                                                                                                                                                                                         | <a href="#">1211</a> , <a href="#">1341</a>                                           |
| Floor                                                        |                                           | geographical redundancy .....                                                                                                                                                                                                                         | <a href="#">126</a>                                                                   |
| Station .....                                                | <a href="#">754</a>                       | Geographical redundancy .....                                                                                                                                                                                                                         | <a href="#">100</a>                                                                   |
| Forwarded Destination .....                                  | <a href="#">756</a>                       | Geographical Redundancy .....                                                                                                                                                                                                                         | <a href="#">109</a> , <a href="#">117</a> , <a href="#">126</a> – <a href="#">128</a> |
| forwarding syslog messages to remote server .....            | <a href="#">1019</a>                      | configuring .....                                                                                                                                                                                                                                     | <a href="#">109</a>                                                                   |
| forward the secondary alarms to primary System Manager ..... | <a href="#">996</a>                       | Geographic Redundancy                                                                                                                                                                                                                                 |                                                                                       |
| FQDN .....                                                   | <a href="#">1509</a>                      | ... <a href="#">113</a> , <a href="#">115</a> , <a href="#">119</a> , <a href="#">120</a> , <a href="#">122</a> , <a href="#">915</a> , <a href="#">916</a> , <a href="#">922</a> , <a href="#">923</a> , <a href="#">1071</a> , <a href="#">1508</a> |                                                                                       |
| changeIPFQDN .....                                           | <a href="#">1510</a>                      | backup and restore .....                                                                                                                                                                                                                              | <a href="#">840</a>                                                                   |
| FQDN and IP address change on Geographic Redundancy .....    | <a href="#">1508</a>                      | disable .....                                                                                                                                                                                                                                         | <a href="#">112</a>                                                                   |
| from web console .....                                       | <a href="#">1274</a>                      | enabling .....                                                                                                                                                                                                                                        | <a href="#">111</a>                                                                   |
| FTP Configuration (F) .....                                  | <a href="#">1305</a>                      | hardware resource or parameter .....                                                                                                                                                                                                                  | <a href="#">101</a>                                                                   |



|                                            |                                           |                                                        |                                             |
|--------------------------------------------|-------------------------------------------|--------------------------------------------------------|---------------------------------------------|
| Geographic Redundancy ( <i>continued</i> ) |                                           | H.320 Desktop Video Conferencing                       | <a href="#">744</a>                         |
| overview                                   | <a href="#">96</a>                        | H323 and SIP passwords                                 | <a href="#">221</a>                         |
| prerequisites                              | <a href="#">100</a>                       | hardware and software prerequisites on primary and     |                                             |
| prerequisite Step 1                        | <a href="#">107</a>                       | secondary servers                                      | <a href="#">100</a>                         |
| prerequisite — Step 2                      | <a href="#">108</a>                       | Hardware support                                       | <a href="#">1476</a>                        |
| Geographic Redundancy field descriptions   | <a href="#">120</a>                       | Harvest Archives page                                  | <a href="#">1015</a>                        |
| Geographic Redundancy key tasks            | <a href="#">103</a>                       | Harvest Criteria Edit page                             | <a href="#">1013</a>                        |
| Geographic Redundancy licenses             | <a href="#">97</a>                        | harvested log files; download                          | <a href="#">1009</a>                        |
| geographic redundancy prerequisites        |                                           | Headset                                                | <a href="#">755</a>                         |
| overview                                   | <a href="#">105</a>                       | health monitor                                         | <a href="#">881</a>                         |
| Geographic Redundancy replication          | <a href="#">100</a>                       | health monitoring                                      |                                             |
| Geographic Redundancy terminology          | <a href="#">98</a>                        | timeout interval                                       | <a href="#">120</a>                         |
| Geo Health                                 | <a href="#">119</a>                       | Health Monitor service                                 | <a href="#">119</a>                         |
| Get                                        |                                           | Hierarchy in communication profile worksheets          | <a href="#">374</a>                         |
| Company ID                                 | <a href="#">1288</a>                      | history                                                |                                             |
| get inventory                              | <a href="#">1443</a>                      | synchronization job                                    | <a href="#">93</a>                          |
| Global Endpoint Change                     | <a href="#">718</a>                       | Holiday After Coverage                                 | <a href="#">702</a>                         |
| global endpoint parameter change           | <a href="#">718</a>                       | Holiday Coverage                                       | <a href="#">702</a>                         |
| global user settings import job            |                                           | Holiday Table                                          | <a href="#">702</a>                         |
| abort                                      | <a href="#">406</a>                       | downloading excel template                             | <a href="#">688</a>                         |
| GLS                                        | <a href="#">159</a>                       | exporting all holiday table                            | <a href="#">686</a>                         |
| graceful shutdown                          | <a href="#">880</a>                       | exporting selected holiday table                       | <a href="#">687</a>                         |
| granular RBAC                              | <a href="#">199</a>                       | importing holiday table                                | <a href="#">687</a>                         |
| GR-aware element                           |                                           | Holiday Table List                                     | <a href="#">686</a>                         |
| manage                                     | <a href="#">916</a>                       | host                                                   | <a href="#">1324</a> , <a href="#">1345</a> |
| GR failover                                | <a href="#">134</a>                       | Host                                                   |                                             |
| GR Health field descriptions               | <a href="#">122</a>                       | update                                                 | <a href="#">1347</a>                        |
| group                                      | <a href="#">834</a> , <a href="#">835</a> | HTTP/HTTPS Configuration (H)                           | <a href="#">1305</a>                        |
| copy                                       | <a href="#">174</a>                       | hunt group                                             |                                             |
| duplicate                                  | <a href="#">174</a>                       | add                                                    | <a href="#">780</a>                         |
| Group and Lookup Service                   | <a href="#">159</a>                       | assign range                                           | <a href="#">213</a>                         |
| Group List                                 | <a href="#">755</a>                       | delete                                                 | <a href="#">781</a>                         |
| Group management                           | <a href="#">159</a>                       | edit                                                   | <a href="#">781</a>                         |
| Group Management page                      | <a href="#">167</a>                       | field-level RBAC                                       | <a href="#">215</a>                         |
| group membership                           | <a href="#">165</a>                       | view                                                   | <a href="#">781</a>                         |
| Group Membership                           | <a href="#">767</a>                       | Hunt Group List                                        |                                             |
| Group Name                                 | <a href="#">196</a>                       | field descriptions                                     | <a href="#">780</a>                         |
| groups                                     |                                           | Hunt Groups                                            | <a href="#">779</a>                         |
| copy                                       | <a href="#">161</a>                       | Hunt-to Station                                        | <a href="#">743</a>                         |
| create                                     | <a href="#">160</a>                       |                                                        |                                             |
| defined                                    | <a href="#">767</a>                       | I                                                      |                                             |
| delete                                     | <a href="#">162</a>                       | identity certificate                                   | <a href="#">1194</a> , <a href="#">1223</a> |
| duplicate                                  | <a href="#">161</a>                       | identity certificates                                  | <a href="#">1192</a>                        |
| filter                                     | <a href="#">165</a>                       | making default                                         | <a href="#">1191</a>                        |
| modify                                     | <a href="#">161</a>                       | renew                                                  | <a href="#">1194</a>                        |
| move                                       | <a href="#">162</a>                       | replacing                                              | <a href="#">1192</a>                        |
| view                                       | <a href="#">160</a>                       | Identity Certificates page                             | <a href="#">1195</a>                        |
| GR-unaware elements                        | <a href="#">131</a>                       | identity certificate updates                           |                                             |
| guidelines                                 |                                           | confirm                                                | <a href="#">1232</a>                        |
| upgrading and updating elements            | <a href="#">1394</a>                      | Idle Appearance Preference                             | <a href="#">751</a>                         |
| guidelines for signing the certificate     |                                           | impact of change in FQDN and IP address on Geographic  |                                             |
| certificate signing request                | <a href="#">1225</a>                      | Redundancy                                             | <a href="#">1508</a>                        |
|                                            |                                           | implicit permissions for Communication Manager objects | <a href="#">200</a>                         |
| <b>H</b>                                   |                                           | implicit permissions for range                         | <a href="#">200</a>                         |
| H.320 Conversion                           |                                           | import                                                 |                                             |
| Attendant Console                          | <a href="#">751</a>                       | elements                                               | <a href="#">944</a>                         |

|                                                                     |                                  |
|---------------------------------------------------------------------|----------------------------------|
| import ( <i>continued</i> )                                         |                                  |
| user data                                                           | <a href="#">370, 376</a>         |
| user data from Excel                                                | <a href="#">370</a>              |
| Import as PEM certificate                                           | <a href="#">1184</a>             |
| import CM station data                                              | <a href="#">370</a>              |
| import CS1000 user data to User Management                          | <a href="#">636</a>              |
| import element;                                                     | <a href="#">898</a>              |
| Import Elements                                                     | <a href="#">944</a>              |
| Import from existing trusted certificates                           | <a href="#">1184</a>             |
| import from file                                                    | <a href="#">1184</a>             |
| Import Global Settings page                                         | <a href="#">584</a>              |
| importing coverage paths                                            | <a href="#">700</a>              |
| importing CS1000 Subscriber Manager data                            | <a href="#">636</a>              |
| importing CS 1000 Subscriber Manager data                           | <a href="#">637, 638</a>         |
| importing CS 1000 user data                                         | <a href="#">637, 639</a>         |
| importing endpoints                                                 | <a href="#">724</a>              |
| importing hunt groups                                               | <a href="#">783</a>              |
| importing the Subscriber Manager data                               | <a href="#">637</a>              |
| importing the user data                                             | <a href="#">634</a>              |
| importing trusted certificates from file                            | <a href="#">1184</a>             |
| importing vector directory numbers                                  | <a href="#">691</a>              |
| import job on the Scheduler page                                    |                                  |
| view                                                                | <a href="#">400</a>              |
| import of users                                                     | <a href="#">379, 391</a>         |
| Import Status page                                                  | <a href="#">946</a>              |
| import the Subscriber Manager data                                  | <a href="#">630, 631</a>         |
| import user                                                         |                                  |
| Excel                                                               | <a href="#">379</a>              |
| XML                                                                 | <a href="#">379</a>              |
| import user considerations                                          | <a href="#">396</a>              |
| import user data to User Management                                 | <a href="#">629</a>              |
| import users                                                        | <a href="#">377</a>              |
| Import Users                                                        | <a href="#">580</a>              |
| Import using TLS                                                    | <a href="#">1184</a>             |
| inactive account deactivation policy field descriptions             | <a href="#">72</a>               |
| Inactive session termination policy                                 | <a href="#">71</a>               |
| incremental synchronization                                         |                                  |
| synchronizing Communication Manager data                            | <a href="#">975</a>              |
| information                                                         |                                  |
| to create Communication Manager                                     | <a href="#">915</a>              |
| to create Messaging                                                 | <a href="#">915</a>              |
| initializing synchronization                                        |                                  |
| synchronizing Communication Manager data                            | <a href="#">975</a>              |
| InSite Knowledge Base                                               | <a href="#">1537</a>             |
| install                                                             |                                  |
| Application Enablement Services                                     | <a href="#">1280</a>             |
| Avaya Aura applications                                             | <a href="#">1280</a>             |
| Avaya Aura Media Server                                             | <a href="#">1280</a>             |
| Avaya Breeze                                                        | <a href="#">1280</a>             |
| Branch Session Manager                                              | <a href="#">1280</a>             |
| Communication Manager                                               | <a href="#">1280</a>             |
| SAL                                                                 | <a href="#">1280</a>             |
| SDM                                                                 | <a href="#">1280</a>             |
| Session Manager                                                     | <a href="#">1280</a>             |
| Solution Deployment Manager client                                  | <a href="#">1280</a>             |
| System Manager                                                      | <a href="#">1280</a>             |
| WebLM                                                               | <a href="#">1280</a>             |
| install custom patches                                              | <a href="#">1399</a>             |
| install custom software patches                                     | <a href="#">1399</a>             |
| Installed Patches                                                   | <a href="#">1401</a>             |
| install FTP server                                                  | <a href="#">1296</a>             |
| Installing and configuring an HTTP server as a remote server        | <a href="#">1295</a>             |
| on a Linux server                                                   | <a href="#">1301</a>             |
| Installing and configuring an SCP or SFTP server as a remote server | <a href="#">1299</a>             |
| installing language pack                                            |                                  |
| Canadian French                                                     | <a href="#">1532</a>             |
| install license file                                                | <a href="#">1033</a>             |
| Install License page                                                | <a href="#">1037</a>             |
| install on same ESXi                                                | <a href="#">1428</a>             |
| install patches                                                     | <a href="#">1357, 1397, 1397</a> |
| install services packs                                              | <a href="#">1357, 1397, 1399</a> |
| install software patches                                            | <a href="#">1357, 1397</a>       |
| Install System Manager patch                                        | <a href="#">1374</a>             |
| Install System Manager patches                                      | <a href="#">1426</a>             |
| Integrated Management transition                                    | <a href="#">1082</a>             |
| Internet Explorer                                                   |                                  |
| compatibility view setting                                          | <a href="#">45</a>               |
| Introduction                                                        | <a href="#">133</a>              |
| inventory                                                           |                                  |
| refresh elements                                                    | <a href="#">1311, 1355</a>       |
| IP address                                                          | <a href="#">1509</a>             |
| IP address and default gateway                                      |                                  |
| changing                                                            | <a href="#">1333</a>             |
| IP address and FQDN change on Geographic Redundancy servers         | <a href="#">1513</a>             |
| IP Audio Hairpinning                                                |                                  |
| Signaling Group                                                     | <a href="#">751</a>              |
| IP Hoteling                                                         | <a href="#">752</a>              |
| IP Office                                                           |                                  |
| add device                                                          | <a href="#">952</a>              |
| delete                                                              | <a href="#">954</a>              |
| reconfigure                                                         | <a href="#">156, 157</a>         |
| synchronization                                                     | <a href="#">972</a>              |
| synchronizing system configuration                                  | <a href="#">976</a>              |
| user management                                                     | <a href="#">156</a>              |
| IP Office; configure                                                | <a href="#">865</a>              |
| IPOffice.properties file                                            |                                  |
| remove association between IP Office endpoint profile and user      | <a href="#">274</a>              |
| IP Office Application Server                                        |                                  |
| synchronize                                                         | <a href="#">977</a>              |
| IP Office configuration                                             | <a href="#">154, 155</a>         |
| IP Office configuring for GR                                        | <a href="#">156</a>              |
| IP Office endpoint profile                                          | <a href="#">271</a>              |
| delete                                                              | <a href="#">273</a>              |
| edit                                                                | <a href="#">272</a>              |
| view                                                                | <a href="#">272</a>              |
| IP Office endpoint template                                         |                                  |
| view                                                                | <a href="#">1141</a>             |
| IP Office endpoint template field description                       | <a href="#">1143</a>             |
| IP Office endpoint templates                                        |                                  |
| add                                                                 | <a href="#">1140</a>             |



IP Office endpoint templates (*continued*)

|                                                             |                      |
|-------------------------------------------------------------|----------------------|
| delete .....                                                | <a href="#">1142</a> |
| edit .....                                                  | <a href="#">1141</a> |
| field description .....                                     | <a href="#">1143</a> |
| remove .....                                                | <a href="#">1142</a> |
| upgrade .....                                               | <a href="#">1143</a> |
| IP Office GR configuration .....                            | <a href="#">154</a>  |
| IP Office GR configuration in Active-Active scenario .....  | <a href="#">156</a>  |
| IP Office GR configuration when primary nonfunctional ..... | <a href="#">156</a>  |
| IP Office profile field description .....                   | <a href="#">865</a>  |
| IP Office System Configuration                              |                      |
| manage audio files .....                                    | <a href="#">1147</a> |
| IP Office system configuration template                     |                      |
| upload audio files .....                                    | <a href="#">1148</a> |
| IP Office System Configuration template                     |                      |
| field descriptions .....                                    | <a href="#">1147</a> |
| IP Office System Configuration template field descriptions  |                      |
| .....                                                       | <a href="#">1147</a> |
| IP Office system configuration templates                    |                      |
| add .....                                                   | <a href="#">1144</a> |
| convert .wav to .c11 .....                                  | <a href="#">1148</a> |
| convert to .c11 .....                                       | <a href="#">1148</a> |
| delete .....                                                | <a href="#">1146</a> |
| delete audio files .....                                    | <a href="#">1149</a> |
| edit .....                                                  | <a href="#">1145</a> |
| view .....                                                  | <a href="#">1145</a> |
| IP Phone Group ID .....                                     | <a href="#">747</a>  |
| IP Softphone .....                                          | <a href="#">752</a>  |
| IP Video .....                                              | <a href="#">750</a>  |

**J**

|                                          |                                             |
|------------------------------------------|---------------------------------------------|
| Jack .....                               | <a href="#">754</a>                         |
| Job Details page .....                   | <a href="#">583</a> , <a href="#">587</a>   |
| Job History .....                        | <a href="#">1386</a> , <a href="#">1391</a> |
| Job Scheduling -Edit Job page .....      | <a href="#">1108</a>                        |
| Job Scheduling -On Demand Job page ..... | <a href="#">1109</a>                        |
| Job Scheduling -View Job page .....      | <a href="#">1106</a>                        |
| job summary                              |                                             |
| synchronization job history .....        | <a href="#">94</a>                          |
| Job summary .....                        | <a href="#">95</a>                          |

**K**

|                                    |                      |
|------------------------------------|----------------------|
| KERBEROS .....                     | <a href="#">1239</a> |
| Kerberos server                    |                      |
| provisioning .....                 | <a href="#">1242</a> |
| Kerberos server provisioning ..... | <a href="#">1242</a> |
| key features                       |                      |
| bulk export .....                  | <a href="#">376</a>  |
| bulk import .....                  | <a href="#">376</a>  |
| key size 2048 .....                | <a href="#">1216</a> |
| key tasks                          |                      |
| Geographic Redundancy .....        | <a href="#">103</a>  |

**L**

|                                                                      |                                             |
|----------------------------------------------------------------------|---------------------------------------------|
| LAC .....                                                            | <a href="#">1032</a>                        |
| LDAP .....                                                           | <a href="#">1239</a>                        |
| LDAP directory server .....                                          | <a href="#">80–82</a> , <a href="#">227</a> |
| LDAP replication .....                                               | <a href="#">100</a>                         |
| LDAP server                                                          |                                             |
| provisioning .....                                                   | <a href="#">54</a> , <a href="#">1241</a>   |
| LDAP server; provision .....                                         | <a href="#">54</a> , <a href="#">1241</a>   |
| LDAP server provisioning .....                                       | <a href="#">54</a> , <a href="#">1241</a>   |
| Library Server Details (L) .....                                     | <a href="#">1305</a>                        |
| License Activation Code .....                                        | <a href="#">1032</a>                        |
| license file .....                                                   | <a href="#">1031</a>                        |
| add mapping .....                                                    | <a href="#">1042</a>                        |
| install .....                                                        | <a href="#">1033</a>                        |
| license file installation .....                                      | <a href="#">1037</a>                        |
| license files and elements .....                                     | <a href="#">1041</a>                        |
| License management .....                                             | <a href="#">143</a>                         |
| License management for Conferencing .....                            | <a href="#">150</a>                         |
| License management for Contact Center .....                          | <a href="#">157</a>                         |
| Licensing                                                            |                                             |
| Geographic Redundancy .....                                          | <a href="#">97</a>                          |
| Life cycle management .....                                          | <a href="#">1316</a>                        |
| limitations                                                          |                                             |
| directory synchronization .....                                      | <a href="#">82</a>                          |
| Limitations of CS 1000 .....                                         | <a href="#">142</a>                         |
| Linkage .....                                                        | <a href="#">702</a>                         |
| Linux-based CS1000 servers                                           |                                             |
| configuration .....                                                  | <a href="#">140</a>                         |
| Linux Operating System upgrades .....                                | <a href="#">1449</a>                        |
| preupgrade check .....                                               | <a href="#">1449</a>                        |
| listing                                                              |                                             |
| slots assignment and encryption passphrase .....                     | <a href="#">1492</a>                        |
| slots assignment and remote key server .....                         | <a href="#">1494</a>                        |
| slots assignment and remote server .....                             | <a href="#">1492</a>                        |
| list of XML Schema Definitions and Sample XMLs for bulk import ..... | <a href="#">408</a>                         |
| list usage extension                                                 |                                             |
| hunt group .....                                                     | <a href="#">782</a>                         |
| list usage extension; announcements .....                            | <a href="#">677</a>                         |
| list usage extension in vector directory number                      |                                             |
| vector directory number; list usage extension .....                  | <a href="#">690</a>                         |
| load AVP host certificate                                            |                                             |
| field descriptions .....                                             | <a href="#">1341</a>                        |
| local data backup                                                    |                                             |
| create .....                                                         | <a href="#">842</a>                         |
| Localized Display Name .....                                         | <a href="#">713</a>                         |
| local software library                                               |                                             |
| configure .....                                                      | <a href="#">1294</a>                        |
| Local Survivable Processor(LSP) .....                                | <a href="#">1305</a>                        |
| local WebLM .....                                                    | <a href="#">1058</a>                        |
| local WebLM server                                                   |                                             |
| remove .....                                                         | <a href="#">1050</a>                        |
| location                                                             |                                             |
| adding .....                                                         | <a href="#">1317</a>                        |
| deleting .....                                                       | <a href="#">1318</a>                        |
| editing .....                                                        | <a href="#">1317</a>                        |

|                                                        |                            |
|--------------------------------------------------------|----------------------------|
| location ( <i>continued</i> )                          |                            |
| view .....                                             | <a href="#">1317</a>       |
| Location .....                                         | <a href="#">740</a>        |
| Locations .....                                        | <a href="#">1386</a>       |
| Lock Messages .....                                    | <a href="#">738</a>        |
| lockout policy                                         |                            |
| password .....                                         | <a href="#">60</a>         |
| Log; log settings .....                                | <a href="#">1017</a>       |
| log details; view .....                                | <a href="#">1023</a>       |
| log file; search for text .....                        | <a href="#">1008</a>       |
| Logged off/PSA/TTI                                     |                            |
| Coverage Path .....                                    | <a href="#">704</a>        |
| logger                                                 |                            |
| edit .....                                             | <a href="#">1018</a>       |
| logging .....                                          | <a href="#">1002</a>       |
| Logging Configuration page .....                       | <a href="#">1017</a>       |
| logging on to System Manager                           |                            |
| administrator privilege .....                          | <a href="#">53</a>         |
| Logging page .....                                     | <a href="#">1024</a>       |
| logging service .....                                  | <a href="#">1002</a>       |
| log harvest; access .....                              | <a href="#">1004</a>       |
| log harvester overview .....                           | <a href="#">1004</a>       |
| Log Harvester page .....                               | <a href="#">1011</a>       |
| log harvesting .....                                   | <a href="#">1004</a>       |
| log harvesting profiles; filter .....                  | <a href="#">1010</a>       |
| log harvest requests; filter .....                     | <a href="#">1010</a>       |
| login details .....                                    | <a href="#">50</a>         |
| login password                                         |                            |
| reset .....                                            | <a href="#">913</a>        |
| login profiles                                         |                            |
| overwrite .....                                        | <a href="#">912</a>        |
| overwriting profiles on devices .....                  | <a href="#">912</a>        |
| log into System Manager .....                          | <a href="#">49</a>         |
| login warning banner .....                             | <a href="#">72, 73</a>     |
| edit .....                                             | <a href="#">73</a>         |
| logo                                                   |                            |
| add .....                                              | <a href="#">74</a>         |
| Logo .....                                             | <a href="#">74</a>         |
| logon banner .....                                     | <a href="#">72</a>         |
| logon information                                      |                            |
| administrator privilege .....                          | <a href="#">53</a>         |
| log on to System Manager                               |                            |
| using EASG login .....                                 | <a href="#">1561</a>       |
| logs; export .....                                     | <a href="#">1023</a>       |
| logs; log viewer .....                                 | <a href="#">1023</a>       |
| logs; search .....                                     | <a href="#">1024</a>       |
| Log Settings .....                                     | <a href="#">1017</a>       |
| logs for Conferencing .....                            | <a href="#">151</a>        |
| Logs Settings service; access .....                    | <a href="#">1017</a>       |
| log types .....                                        | <a href="#">1003</a>       |
| log viewer .....                                       | <a href="#">1002</a>       |
| Log Viewer .....                                       | <a href="#">1023</a>       |
| Loss Group .....                                       | <a href="#">745</a>        |
| LWC Activation .....                                   | <a href="#">752</a>        |
| LWC Log External Calls .....                           | <a href="#">752</a>        |
| LWC Reception                                          |                            |
| Agent Login ID .....                                   | <a href="#">745</a>        |
| <b>M</b>                                               |                            |
| MAC address of server .....                            | <a href="#">1045</a>       |
| mailbox administration                                 |                            |
| subscriber management .....                            | <a href="#">640</a>        |
| Mailing reports .....                                  | <a href="#">1092</a>       |
| maintenance                                            |                            |
| clear amw all .....                                    | <a href="#">722</a>        |
| making default certificate .....                       | <a href="#">1191</a>       |
| making the new CA as default System Manager CA         |                            |
| command MakeNewCADefault .....                         | <a href="#">1220</a>       |
| using option 2 .....                                   | <a href="#">1220</a>       |
| manage                                                 |                            |
| applications .....                                     | <a href="#">896</a>        |
| elements .....                                         | <a href="#">896</a>        |
| GR-aware element .....                                 | <a href="#">916</a>        |
| identity certificate .....                             | <a href="#">1194</a>       |
| tenant .....                                           | <a href="#">1259, 1260</a> |
| trusted certificate .....                              | <a href="#">1189</a>       |
| Manage                                                 |                            |
| System Manager upgrades .....                          | <a href="#">1426</a>       |
| manage applications .....                              | <a href="#">896</a>        |
| manage audio field description .....                   | <a href="#">1149</a>       |
| manage certificate revocation field descriptions ..... | <a href="#">1198</a>       |
| manage certificates .....                              | <a href="#">1178</a>       |
| managed elements                                       |                            |
| changing System Manager IP address .....               | <a href="#">1512</a>       |
| manage elements .....                                  | <a href="#">896, 922</a>   |
| Geographic Redundancy .....                            | <a href="#">915</a>        |
| Manage Elements field descriptions .....               | <a href="#">933</a>        |
| manage entity classes .....                            | <a href="#">1200</a>       |
| Manage Entity Classes                                  |                            |
| field descriptions .....                               | <a href="#">1202</a>       |
| Management interface .....                             | <a href="#">1505</a>       |
| manage Presence access control lists .....             | <a href="#">608</a>        |
| manage public contact list .....                       | <a href="#">593</a>        |
| manage resources .....                                 | <a href="#">175</a>        |
| manage shared address .....                            | <a href="#">604</a>        |
| Manage Software .....                                  | <a href="#">1392</a>       |
| manage software library files field description .....  | <a href="#">1309</a>       |
| manage users .....                                     | <a href="#">219</a>        |
| managing                                               |                            |
| password policy through CLI .....                      | <a href="#">65</a>         |
| Managing                                               |                            |
| outbound firewall rule logging .....                   | <a href="#">1177</a>       |
| managing certificates migrated hosts .....             | <a href="#">1350</a>       |
| managing certification authorities .....               | <a href="#">1222</a>       |
| Managing NRP .....                                     | <a href="#">836</a>        |
| Managing NRP groups .....                              | <a href="#">836</a>        |
| Managing outbound firewall rule logging .....          | <a href="#">1177</a>       |
| managing resources .....                               | <a href="#">175</a>        |
| managing SNMPv3 user profiles .....                    | <a href="#">967, 969</a>   |
| managing target profiles .....                         | <a href="#">968</a>        |
| managing tasks after running createCA utility .....    | <a href="#">1222</a>       |
| managing user profiles .....                           | <a href="#">969</a>        |
| managing users .....                                   | <a href="#">1290</a>       |
| Manual addition of elements .....                      | <a href="#">898</a>        |

|                                                            |                                                                    |  |
|------------------------------------------------------------|--------------------------------------------------------------------|--|
| map                                                        |                                                                    |  |
| permission                                                 | <a href="#">197</a>                                                |  |
| permission from template                                   | <a href="#">197</a>                                                |  |
| map ESXi host to unknown location                          | <a href="#">1339</a>                                               |  |
| map permission                                             | <a href="#">193</a>                                                |  |
| map permissions                                            |                                                                    |  |
| using templates                                            | <a href="#">191</a>                                                |  |
| mapping                                                    |                                                                    |  |
| add                                                        | <a href="#">196</a>                                                |  |
| mapping elements and license files                         | <a href="#">1041</a>                                               |  |
| Map-to Station                                             | <a href="#">743</a>                                                |  |
| Map vCenter                                                | <a href="#">1378</a> , <a href="#">1380</a> , <a href="#">1381</a> |  |
| Media Complex Ext                                          | <a href="#">746</a>                                                |  |
| media server                                               | <a href="#">679</a>                                                |  |
| Meeting Exchange configuration                             | <a href="#">143</a>                                                |  |
| Meeting Exchange element configuration                     | <a href="#">143</a>                                                |  |
| memory requirement                                         | <a href="#">1450</a>                                               |  |
| Message Lamp Ext                                           | <a href="#">737</a>                                                |  |
| messaging class of service                                 | <a href="#">639</a>                                                |  |
| Messaging configuration                                    | <a href="#">144</a>                                                |  |
| Messaging configuration in GR failback                     | <a href="#">146</a>                                                |  |
| Messaging configuration in operational mode                | <a href="#">145</a>                                                |  |
| Messaging configuration in split network                   | <a href="#">147</a>                                                |  |
| Messaging configuration when primary is nonoperational     | <a href="#">145</a>                                                |  |
| messaging COS                                              | <a href="#">639</a>                                                |  |
| messaging data                                             |                                                                    |  |
| synchronize                                                | <a href="#">978</a>                                                |  |
| Messaging data                                             | <a href="#">972</a>                                                |  |
| Messaging field description                                | <a href="#">1132</a>                                               |  |
| Messaging field descriptions                               |                                                                    |  |
| add subscriber                                             | <a href="#">643</a>                                                |  |
| Messaging profile                                          |                                                                    |  |
| edit                                                       | <a href="#">871</a>                                                |  |
| view                                                       | <a href="#">871</a>                                                |  |
| Metering Collector configuration                           |                                                                    |  |
| overview                                                   | <a href="#">1068</a>                                               |  |
| MIB.properties                                             | <a href="#">955</a>                                                |  |
| MIB tool                                                   | <a href="#">955</a> , <a href="#">956</a>                          |  |
| MIBTOOL.jar                                                | <a href="#">955</a>                                                |  |
| MIBXMLTAGS.properties                                      | <a href="#">955</a>                                                |  |
| Microsoft Active Directory certificate                     | <a href="#">1183</a>                                               |  |
| migrate                                                    |                                                                    |  |
| System Platform-based system and elements in bulk to       |                                                                    |  |
| AVP remotely                                               | <a href="#">1418</a>                                               |  |
| migrated hosts                                             |                                                                    |  |
| managing certificates                                      | <a href="#">1350</a>                                               |  |
| migrating                                                  |                                                                    |  |
| 96x1 SIP set type to J1xx endpoint                         | <a href="#">728</a>                                                |  |
| all 96x1 SIP to J1xx set type                              | <a href="#">730</a>                                                |  |
| System Platform-based system and elements to AVP           |                                                                    |  |
| remotely                                                   | <a href="#">1414</a>                                               |  |
| Migration of J-Series endpoints configured as 96x1 SIP set |                                                                    |  |
| type                                                       | <a href="#">725</a>                                                |  |
| modify                                                     |                                                                    |  |
| element access profile                                     | <a href="#">911</a>                                                |  |
| port                                                       | <a href="#">922</a>                                                |  |
| Modify Access Profile Entry                                | <a href="#">911</a>                                                |  |
| modify appender                                            | <a href="#">1020</a>                                               |  |
| modify details of a private contact                        | <a href="#">281</a>                                                |  |
| modify details of a public contact                         | <a href="#">594</a>                                                |  |
| modify element                                             | <a href="#">917</a>                                                |  |
| modify FQDN                                                |                                                                    |  |
| primary System Manager                                     | <a href="#">1514</a>                                               |  |
| secondary System Manager                                   | <a href="#">1515</a>                                               |  |
| Modify FQDN                                                |                                                                    |  |
| secondary System Manager                                   | <a href="#">1516</a>                                               |  |
| modifying                                                  |                                                                    |  |
| communication address                                      | <a href="#">259</a>                                                |  |
| user provisioning rule                                     | <a href="#">616</a>                                                |  |
| modifying, user address                                    | <a href="#">254</a>                                                |  |
| modifying a CM Endpoint profile                            | <a href="#">264</a>                                                |  |
| modifying a contact address of a private contact           | <a href="#">285</a>                                                |  |
| modifying a CS 1000 profile                                | <a href="#">270</a>                                                |  |
| modifying a local WebLM server configuration               | <a href="#">1049</a>                                               |  |
| modifying a managed element's IP address and FQDN          | <a href="#">1512</a>                                               |  |
| modifying a messaging profile                              | <a href="#">267</a>                                                |  |
| modifying an access profile                                | <a href="#">921</a>                                                |  |
| modifying an appender                                      | <a href="#">1020</a>                                               |  |
| modifying an IP Office endpoint profile                    | <a href="#">272</a>                                                |  |
| modifying a port                                           | <a href="#">922</a>                                                |  |
| modifying a postal address of a public contact             | <a href="#">595</a>                                                |  |
| modifying a shared address                                 | <a href="#">605</a>                                                |  |
| modifying contact in a contact list                        | <a href="#">275</a>                                                |  |
| modifying default end entities                             | <a href="#">1230</a>                                               |  |
| modifying groups                                           | <a href="#">161</a>                                                |  |
| modifying postal address of a private contact              | <a href="#">283</a>                                                |  |
| modifying SNMPv3 user profiles                             | <a href="#">957</a>                                                |  |
| modifying the communication address                        | <a href="#">259</a>                                                |  |
| modifying the details of a public contact                  | <a href="#">597</a>                                                |  |
| modifying user account                                     | <a href="#">230</a>                                                |  |
| modifying user provisioning rule                           | <a href="#">616</a>                                                |  |
| modify IP address                                          |                                                                    |  |
| primary System Manager                                     | <a href="#">1514</a>                                               |  |
| secondary System Manager                                   | <a href="#">1515</a> , <a href="#">1516</a>                        |  |
| Modify local WebLM page                                    | <a href="#">1059</a>                                               |  |
| monitoring                                                 |                                                                    |  |
| application                                                | <a href="#">1377</a>                                               |  |
| platform                                                   | <a href="#">1377</a>                                               |  |
| Mounting                                                   | <a href="#">754</a>                                                |  |
| Move Group page                                            | <a href="#">174</a>                                                |  |
| move primary System Manager server                         | <a href="#">126</a> , <a href="#">127</a>                          |  |
| moving an announcement                                     | <a href="#">675</a>                                                |  |
| moving announcements                                       | <a href="#">675</a>                                                |  |
| moving groups                                              | <a href="#">162</a>                                                |  |
| MPC firmware                                               |                                                                    |  |
| update                                                     | <a href="#">1486</a>                                               |  |
| multibyte language                                         | <a href="#">738</a>                                                |  |
| Multi Device Access                                        | <a href="#">261</a>                                                |  |
| Multimedia Early Answer                                    | <a href="#">752</a>                                                |  |
| Multimedia Messaging                                       | <a href="#">158</a>                                                |  |
| multiple SIP endpoints                                     |                                                                    |  |
| register                                                   | <a href="#">261</a>                                                |  |
| multiple users                                             |                                                                    |  |
| assign groups                                              | <a href="#">252</a>                                                |  |

|                                                       |                                                                                           |                                                        |                      |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------|----------------------|
| Multi Tenancy .....                                   | <a href="#">1254</a> , <a href="#">1256</a> , <a href="#">1259</a> – <a href="#">1261</a> | Notification filtering .....                           | <a href="#">962</a>  |
| Avaya SIP AST endpoints .....                         | <a href="#">1263</a>                                                                      | notification filter profile                            |                      |
| Communication Manager .....                           | <a href="#">1263</a> , <a href="#">1264</a>                                               | create .....                                           | <a href="#">963</a>  |
| enable .....                                          | <a href="#">874</a>                                                                       | delete .....                                           | <a href="#">964</a>  |
| enabling .....                                        | <a href="#">1255</a>                                                                      | edit .....                                             | <a href="#">964</a>  |
| RBAC .....                                            | <a href="#">1264</a>                                                                      | view .....                                             | <a href="#">963</a>  |
| scheduler .....                                       | <a href="#">1264</a>                                                                      | Notification Filter Profiles                           |                      |
| user management .....                                 | <a href="#">1264</a>                                                                      | field descriptions .....                               | <a href="#">966</a>  |
| user provisioning rule .....                          | <a href="#">1264</a>                                                                      | notification ID .....                                  | <a href="#">963</a>  |
| Multi Tenancy for Communication Manager .....         | <a href="#">1264</a>                                                                      | notification IDs .....                                 | <a href="#">966</a>  |
| Multi Tenancy for Communication Manager objects ..... | <a href="#">1263</a>                                                                      | notify sync feature .....                              | <a href="#">1497</a> |
| Music SourceMusic Source .....                        | <a href="#">754</a>                                                                       | notify sync on Communication Manager .....             | <a href="#">1501</a> |
| Mute Button Enabled .....                             | <a href="#">752</a>                                                                       | NRP groups .....                                       | <a href="#">836</a>  |
| MWI Served User Type .....                            | <a href="#">741</a>                                                                       | NRP sync .....                                         | <a href="#">835</a>  |
| My Docs .....                                         | <a href="#">1535</a>                                                                      | NRP sync feature .....                                 | <a href="#">835</a>  |
| <b>N</b>                                              |                                                                                           | NTP server                                             |                      |
| native name .....                                     | <a href="#">713</a>                                                                       | configure .....                                        | <a href="#">1530</a> |
| network parameters                                    |                                                                                           | Number of Rings .....                                  | <a href="#">704</a>  |
| change .....                                          | <a href="#">1344</a>                                                                      | <b>O</b>                                               |                      |
| new                                                   |                                                                                           | Obtaining Microsoft Active Directory certificate ..... | <a href="#">1183</a> |
| role .....                                            | <a href="#">195</a>                                                                       | obtain the license file .....                          | <a href="#">1031</a> |
| new CRL                                               |                                                                                           | Officelinx                                             |                      |
| creation .....                                        | <a href="#">1233</a>                                                                      | adding to System Manager .....                         | <a href="#">929</a>  |
| New Element page .....                                | <a href="#">936</a>                                                                       | Off PBX Configuration Set                              |                      |
| New Group page .....                                  | <a href="#">168</a>                                                                       | Edit .....                                             | <a href="#">787</a>  |
| new identity certificates                             |                                                                                           | field description .....                                | <a href="#">787</a>  |
| System Manager .....                                  | <a href="#">1232</a>                                                                      | View .....                                             | <a href="#">786</a>  |
| new in release                                        |                                                                                           | Off PBX Configuration Set field descriptions .....     | <a href="#">787</a>  |
| System Manager 8.1 .....                              | <a href="#">42</a>                                                                        | Off PBX endpoint mapping                               |                      |
| new in release 8.1.1                                  |                                                                                           | add .....                                              | <a href="#">789</a>  |
| System Manager .....                                  | <a href="#">41</a>                                                                        | Off PBX Endpoint Mapping                               |                      |
| new in release 8.1.2                                  |                                                                                           | edit .....                                             | <a href="#">790</a>  |
| System Manager .....                                  | <a href="#">41</a>                                                                        | field description .....                                | <a href="#">790</a>  |
| new in release 8.1.3                                  |                                                                                           | view .....                                             | <a href="#">790</a>  |
| System Manager .....                                  | <a href="#">39</a>                                                                        | Off PBX Endpoint Mapping field description .....       | <a href="#">790</a>  |
| new in release 8.1.3.1                                |                                                                                           | on-demand job .....                                    | <a href="#">1096</a> |
| System Manager .....                                  | <a href="#">38</a>                                                                        | optional settings                                      |                      |
| New Location .....                                    | <a href="#">1318</a>                                                                      | security hardening .....                               | <a href="#">1165</a> |
| New Private Contact List page .....                   | <a href="#">286</a>                                                                       | Out of Band Management .....                           | <a href="#">1505</a> |
| new profile                                           |                                                                                           | disable .....                                          | <a href="#">1506</a> |
| create .....                                          | <a href="#">234</a>                                                                       | enable .....                                           | <a href="#">1506</a> |
| New Public Contact List page .....                    | <a href="#">601</a>                                                                       | Geographic Redundancy .....                            | <a href="#">1507</a> |
| new reports .....                                     | <a href="#">1085</a>                                                                      | overview                                               |                      |
| new root CA                                           |                                                                                           | extended hostname validation .....                     | <a href="#">1239</a> |
| downloading .....                                     | <a href="#">1218</a>                                                                      | geographical redundancy .....                          | <a href="#">105</a>  |
| new subscriber                                        |                                                                                           | Overview .....                                         | <a href="#">131</a>  |
| templates .....                                       | <a href="#">1121</a>                                                                      | overview of System Manager root certificate authority  |                      |
| New User Provisioning Rule                            |                                                                                           | using SHA256withRSA signing algorithm and 2048 key     |                      |
| field descriptions .....                              | <a href="#">619</a>                                                                       | size .....                                             | <a href="#">1215</a> |
| new users; add .....                                  | <a href="#">1290</a>                                                                      | Overwrite the existing outbound firewall rules .....   | <a href="#">1176</a> |
| New vCenter .....                                     | <a href="#">1381</a>                                                                      | overwriting                                            |                      |
| Next Path Number .....                                | <a href="#">702</a>                                                                       | existing outbound firewall rules .....                 | <a href="#">1176</a> |
| non sip endpoints .....                               | <a href="#">777</a>                                                                       | overwriting login profiles .....                       | <a href="#">912</a>  |
| non-station objects; view                             |                                                                                           |                                                        |                      |
| Communication Manager objects; view .....             | <a href="#">656</a>                                                                       |                                                        |                      |

**P**

|                                                         |                                                                   |                                                                                   |                                             |
|---------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------|
| parameters .....                                        | <a href="#">1088</a>                                              | port matrix .....                                                                 | <a href="#">1534</a>                        |
| parent group .....                                      | <a href="#">180</a>                                               | post login banner message .....                                                   | <a href="#">73</a>                          |
| password .....                                          |                                                                   | post operations after running CreateCA utility .....                              | <a href="#">1222</a>                        |
| change .....                                            | <a href="#">1346</a>                                              | Precedence Call Waiting .....                                                     | <a href="#">753</a>                         |
| Password aging policy enforcement .....                 | <a href="#">59</a>                                                | preferred languages .....                                                         | <a href="#">90</a>                          |
| password change .....                                   |                                                                   | preparing CS 1000 Subscriber Manager data for import to<br>System Manager .....   | <a href="#">637</a>                         |
| Appliance Virtualization Platform host .....            | <a href="#">1327</a>                                              | prerequisite .....                                                                |                                             |
| password history enforcement policy .....               | <a href="#">60</a>                                                | Geographic Redundancy Step 1 .....                                                | <a href="#">107</a>                         |
| password lockout policy enforcement .....               | <a href="#">60</a>                                                | Geographic Redundancy — Step 2 .....                                              | <a href="#">108</a>                         |
| password policies .....                                 |                                                                   | prerequisites .....                                                               | <a href="#">100</a> , <a href="#">103</a>   |
| edit .....                                              | <a href="#">60</a>                                                | prerequisites before making the new root CA as default ..                         | <a href="#">1218</a>                        |
| password policies field description .....               | <a href="#">61</a>                                                | Presence access control lists (ACLs) .....                                        | <a href="#">608</a>                         |
| password policy .....                                   | <a href="#">610</a> , <a href="#">1327</a> , <a href="#">1328</a> | Presence ACL .....                                                                | <a href="#">608</a>                         |
| communication profile .....                             | <a href="#">609</a>                                               | Presence communication profile administration .....                               | <a href="#">262</a>                         |
| password rules .....                                    | <a href="#">1328</a>                                              | Presence Server .....                                                             |                                             |
| password strength policy enforcement .....              | <a href="#">60</a>                                                | configuration .....                                                               | <a href="#">143</a> , <a href="#">144</a>   |
| peak usage; view .....                                  | <a href="#">1035</a>                                              | Pre-Upgrade .....                                                                 | <a href="#">1448</a>                        |
| peak usage for a licensed product .....                 | <a href="#">1035</a>                                              | preupgrade check .....                                                            | <a href="#">1449</a>                        |
| pending jobs .....                                      |                                                                   | applications .....                                                                | <a href="#">1314</a>                        |
| view .....                                              | <a href="#">1099</a>                                              | Pre-Upgrade Check .....                                                           | <a href="#">1446</a> , <a href="#">1448</a> |
| pending jobs; stop .....                                | <a href="#">1102</a>                                              | pre upgrade checks .....                                                          |                                             |
| pending jobs; view .....                                | <a href="#">1098</a>                                              | System Platform upgrades .....                                                    | <a href="#">1449</a>                        |
| Pending Jobs page .....                                 | <a href="#">1103</a>                                              | Preupgrade Configuration .....                                                    | <a href="#">1314</a>                        |
| Per Button Ring Control .....                           | <a href="#">752</a>                                               | preupgrade job status .....                                                       | <a href="#">1436</a>                        |
| performing .....                                        |                                                                   | preupgrade status .....                                                           | <a href="#">1451</a>                        |
| Pre-Upgrade Check .....                                 | <a href="#">1446</a>                                              | primary server .....                                                              |                                             |
| Performing a CM Audit .....                             | <a href="#">979</a>                                               | CRL addition .....                                                                | <a href="#">124</a>                         |
| Periodic cleanup of reports .....                       | <a href="#">869</a>                                               | primary Session Manager .....                                                     | <a href="#">739</a>                         |
| Periodic Status .....                                   | <a href="#">1067</a>                                              | primary System Manager .....                                                      |                                             |
| periodic status of master and local WebLM servers ..... | <a href="#">1052</a>                                              | change FQDN .....                                                                 | <a href="#">1513</a>                        |
| permission .....                                        |                                                                   | change IP address .....                                                           | <a href="#">1513</a>                        |
| copy .....                                              | <a href="#">197</a>                                               | private contact .....                                                             |                                             |
| map .....                                               | <a href="#">197</a>                                               | add a contact address .....                                                       | <a href="#">284</a>                         |
| permission mapping .....                                | <a href="#">191</a> , <a href="#">197</a>                         | modify details .....                                                              | <a href="#">281</a>                         |
| permissions .....                                       |                                                                   | Private Contact .....                                                             | <a href="#">286</a>                         |
| Scheduler .....                                         | <a href="#">1097</a>                                              | Problems in managing Session Manager 6.1 or 6.2 using<br>System Manager 6.2 ..... | <a href="#">135</a>                         |
| Solution Deployment Manager .....                       | <a href="#">190</a>                                               | Profile .....                                                                     | <a href="#">760</a>                         |
| Personalized Ringing Pattern .....                      | <a href="#">742</a>                                               | Profile Criteria View page .....                                                  | <a href="#">1013</a>                        |
| Personal List .....                                     | <a href="#">755</a>                                               | profiles .....                                                                    |                                             |
| Per Station CPN - Send Calling Number .....             | <a href="#">741</a>                                               | discovery .....                                                                   | <a href="#">899</a>                         |
| phone view layout .....                                 |                                                                   | Profiles .....                                                                    | <a href="#">1246</a>                        |
| read only phone view .....                              | <a href="#">757</a>                                               | Profile Settings .....                                                            | <a href="#">760</a>                         |
| platform .....                                          |                                                                   | Protocol consideration .....                                                      | <a href="#">1247</a>                        |
| editing .....                                           | <a href="#">1321</a>                                              | protocol matrix for upgrades .....                                                | <a href="#">1486</a>                        |
| monitoring .....                                        | <a href="#">1377</a>                                              | protocol requirements to configure remote server .....                            | <a href="#">1294</a>                        |
| Platforms .....                                         | <a href="#">1386</a>                                              | protocol support .....                                                            |                                             |
| PLDS .....                                              |                                                                   | software library .....                                                            | <a href="#">1294</a>                        |
| finding LAC .....                                       | <a href="#">1032</a>                                              | provision .....                                                                   |                                             |
| PLDS access .....                                       | <a href="#">1287</a>                                              | users .....                                                                       | <a href="#">613</a>                         |
| PLDS access to Avaya .....                              | <a href="#">1287</a>                                              | provisioning .....                                                                |                                             |
| Point1, Point2, ... ..                                  | <a href="#">704</a>                                               | authentication servers .....                                                      | <a href="#">1241</a>                        |
| port .....                                              |                                                                   | Kerberos server .....                                                             | <a href="#">1242</a>                        |
| modify .....                                            | <a href="#">922</a>                                               | LDAP server .....                                                                 | <a href="#">54</a> , <a href="#">1241</a>   |
| Port .....                                              | <a href="#">936</a>                                               | RADIUS server .....                                                               | <a href="#">1242</a>                        |
| Station .....                                           | <a href="#">736</a>                                               | user certificate authentication .....                                             | <a href="#">1243</a>                        |

|                                                    |                                           |                                                                      |                                             |
|----------------------------------------------------|-------------------------------------------|----------------------------------------------------------------------|---------------------------------------------|
| provisioning authentication servers .....          | <a href="#">1241</a>                      | reconfiguring IP Office .....                                        | <a href="#">156</a>                         |
| provisioning Kerberos server .....                 | <a href="#">1242</a>                      | reconfiguring Visualization, Performance, and Fault Manager .....    | <a href="#">157</a>                         |
| provisioning LDAP server .....                     | <a href="#">54</a> , <a href="#">1241</a> | recover primary server from disaster .....                           | <a href="#">129</a>                         |
| provisioning RADIUS server .....                   | <a href="#">1242</a>                      | redirect                                                             |                                             |
| provisioning user certificate authentication ..... | <a href="#">1243</a>                      | CS 1000 user to Element Manager .....                                | <a href="#">269</a>                         |
| provision Remote Identity Provider .....           | <a href="#">1249</a>                      | redirecting CS 1000 to Element Manager .....                         | <a href="#">269</a>                         |
| public contact                                     |                                           | Redirect Notification .....                                          | <a href="#">753</a>                         |
| add .....                                          | <a href="#">593</a>                       | reestablish                                                          |                                             |
| add contact address .....                          | <a href="#">596</a>                       | connection .....                                                     | <a href="#">1374</a>                        |
| add postal address .....                           | <a href="#">595</a>                       | Reestablish Connection .....                                         | <a href="#">1386</a>                        |
| choose a shared address .....                      | <a href="#">596</a>                       | re-establishing trust                                                |                                             |
| delete .....                                       | <a href="#">594</a>                       | application .....                                                    | <a href="#">1356</a>                        |
| delete contact address .....                       | <a href="#">597</a>                       | SDM elements .....                                                   | <a href="#">1356</a>                        |
| delete the postal address .....                    | <a href="#">596</a>                       | Solution Deployment Manager elements .....                           | <a href="#">1356</a>                        |
| modify details .....                               | <a href="#">594</a>                       | re-establishing trust application .....                              | <a href="#">1356</a>                        |
| view details .....                                 | <a href="#">594</a>                       | refresh elements in inventory .....                                  | <a href="#">1311</a> , <a href="#">1355</a> |
| public contacts .....                              | <a href="#">219</a> , <a href="#">602</a> | refresh elements job status .....                                    | <a href="#">1436</a>                        |
| Public Contacts                                    |                                           | refreshing                                                           |                                             |
| field descriptions .....                           | <a href="#">597</a>                       | default password policy settings .....                               | <a href="#">70</a>                          |
| Public interface .....                             | <a href="#">1505</a>                      | refreshing the default password policy settings .....                | <a href="#">70</a>                          |
| push                                               |                                           | regenerating                                                         |                                             |
| login banner on host .....                         | <a href="#">1338</a>                      | asymmetric keys .....                                                | <a href="#">1252</a>                        |
| pushing                                            |                                           | symmetric keys .....                                                 | <a href="#">1251</a>                        |
| syslog .....                                       | <a href="#">1384</a>                      | regenerating asymmetric keys                                         |                                             |
|                                                    |                                           | geographic redundancy disabled .....                                 | <a href="#">1252</a>                        |
|                                                    |                                           | geographic redundancy enabled .....                                  | <a href="#">1252</a>                        |
|                                                    |                                           | regenerating symmetric keys .....                                    | <a href="#">1251</a>                        |
|                                                    |                                           | register                                                             |                                             |
|                                                    |                                           | multiple SIP endpoints .....                                         | <a href="#">261</a>                         |
|                                                    |                                           | Reimporting SSO cookie domain value .....                            | <a href="#">75</a>                          |
|                                                    |                                           | releasing endpoint .....                                             | <a href="#">721</a>                         |
|                                                    |                                           | remote access                                                        |                                             |
|                                                    |                                           | System Manager CLI .....                                             | <a href="#">1560</a>                        |
|                                                    |                                           | System Manager web console .....                                     | <a href="#">1560</a>                        |
|                                                    |                                           | remote backup server supported                                       |                                             |
|                                                    |                                           | ciphers .....                                                        | <a href="#">851</a>                         |
|                                                    |                                           | key exchange algorithms .....                                        | <a href="#">851</a>                         |
|                                                    |                                           | mac algorithms .....                                                 | <a href="#">851</a>                         |
|                                                    |                                           | Remote Identity Provider .....                                       | <a href="#">1248</a>                        |
|                                                    |                                           | Remote Identity Provider; provision .....                            | <a href="#">1249</a>                        |
|                                                    |                                           | remote library .....                                                 | <a href="#">1305</a>                        |
|                                                    |                                           | Remote Off-hook Attempt .....                                        | <a href="#">772</a>                         |
|                                                    |                                           | remote server                                                        |                                             |
|                                                    |                                           | forward syslog messages .....                                        | <a href="#">1019</a>                        |
|                                                    |                                           | Remote Server                                                        |                                             |
|                                                    |                                           | add .....                                                            | <a href="#">1093</a>                        |
|                                                    |                                           | delete .....                                                         | <a href="#">1094</a>                        |
|                                                    |                                           | edit .....                                                           | <a href="#">1094</a>                        |
|                                                    |                                           | view details .....                                                   | <a href="#">1093</a>                        |
|                                                    |                                           | Remote Soft Phone Emergency Calls .....                              | <a href="#">743</a>                         |
|                                                    |                                           | remove assigned elements .....                                       | <a href="#">920</a>                         |
|                                                    |                                           | remove association between IP Office endpoint profile and user ..... | <a href="#">274</a>                         |
|                                                    |                                           | remove a user from groups .....                                      | <a href="#">252</a>                         |
|                                                    |                                           | remove endpoint dependencies                                         |                                             |
|                                                    |                                           | field description .....                                              | <a href="#">833</a>                         |

## Q

|                                                                             |                      |
|-----------------------------------------------------------------------------|----------------------|
| querying usage of feature licenses for master and local WebLM servers ..... | <a href="#">1053</a> |
| Query Usage page .....                                                      | <a href="#">1064</a> |
| Quick Navigator .....                                                       | <a href="#">46</a>   |
| quick start to importing users .....                                        | <a href="#">587</a>  |

## R

|                                                          |                                           |
|----------------------------------------------------------|-------------------------------------------|
| RADIUS .....                                             | <a href="#">1239</a>                      |
| RADIUS server                                            |                                           |
| provisioning .....                                       | <a href="#">1242</a>                      |
| range .....                                              | <a href="#">199</a>                       |
| endpoints .....                                          | <a href="#">209</a>                       |
| Range in endpoints .....                                 | <a href="#">208</a>                       |
| RBAC .....                                               | <a href="#">181</a>                       |
| built-in roles .....                                     | <a href="#">182</a>                       |
| custom roles .....                                       | <a href="#">186</a>                       |
| RBAC for Conferencing .....                              | <a href="#">150</a>                       |
| Ready for Upgrade .....                                  | <a href="#">1466</a>                      |
| reboot .....                                             | <a href="#">1274</a>                      |
| reboot System Manager .....                              | <a href="#">1274</a>                      |
| Re-Calculate route pattern .....                         | <a href="#">832</a>                       |
| receiving certificate response .....                     | <a href="#">1226</a>                      |
| reconfiguring Conferencing .....                         | <a href="#">151</a>                       |
| reconfiguring Conferencing .....                         | <a href="#">150</a> , <a href="#">151</a> |
| reconfiguring IP address and FQDN for Conferencing ..... | <a href="#">150</a>                       |
| reconfigure Conferencing .....                           | <a href="#">151</a>                       |
| reconfiguring AES .....                                  | <a href="#">157</a>                       |
| reconfiguring Conferencing .....                         | <a href="#">150</a>                       |
| reconfiguring Contact Center .....                       | <a href="#">157</a>                       |



|                                                           |                                             |                                                       |                         |
|-----------------------------------------------------------|---------------------------------------------|-------------------------------------------------------|-------------------------|
| remove endpoint reference field description .....         | <a href="#">833</a>                         | Re run                                                |                         |
| remove replica node from queue .....                      | <a href="#">1074</a>                        | reports .....                                         | <a href="#">1088</a>    |
| remove roles .....                                        | <a href="#">251</a>                         | Re running reports .....                              | <a href="#">1088</a>    |
| remove user account .....                                 | <a href="#">232</a>                         | resetting the password .....                          | <a href="#">913</a>     |
| removing                                                  |                                             | resolving anonymous profiles .....                    | <a href="#">982</a>     |
| Appliance Virtualization Platform host .....              | <a href="#">1337</a>                        | resources                                             |                         |
| encryption passphrase .....                               | <a href="#">1492</a>                        | assign to group .....                                 | <a href="#">176</a>     |
| ESXi host .....                                           | <a href="#">1337</a>                        | filter .....                                          | <a href="#">166</a>     |
| outbound firewall rules .....                             | <a href="#">1175</a>                        | group .....                                           | <a href="#">163</a>     |
| remote key server .....                                   | <a href="#">1494</a>                        | manage .....                                          | <a href="#">175</a>     |
| removing additional identity certificates .....           | <a href="#">1192</a>                        | remove .....                                          | <a href="#">167</a>     |
| removing an appender from a logger .....                  | <a href="#">1020</a>                        | search .....                                          | <a href="#">164</a>     |
| removing an association between a subscriber and a user   |                                             | search group .....                                    | <a href="#">165</a>     |
| .....                                                     | <a href="#">268</a>                         | resources; filter .....                               | <a href="#">177</a>     |
| removing a node .....                                     | <a href="#">1074</a>                        | resources; search .....                               | <a href="#">177</a>     |
| removing assigned resources from group .....              | <a href="#">167</a>                         | resources; synchronize .....                          | <a href="#">163</a>     |
| removing association between an endpoint and a user ..... | <a href="#">265</a>                         | Resources page .....                                  | <a href="#">178</a>     |
| removing deleted users from database .....                | <a href="#">232</a>                         | Resource Synchronization page .....                   | <a href="#">175</a>     |
| removing dependencies of endpoints .....                  | <a href="#">833</a>                         | restart                                               |                         |
| removing local WebLM server .....                         | <a href="#">1050</a>                        | application .....                                     | <a href="#">1361</a>    |
| removing location from host .....                         | <a href="#">1380</a>                        | restart application from SDM .....                    | <a href="#">1361</a>    |
| removing outbound firewall rules .....                    | <a href="#">1175</a>                        | restarting                                            |                         |
| removing references to endpoints .....                    | <a href="#">833</a>                         | Appliance Virtualization Platform .....               | <a href="#">1337</a>    |
| removing trusted certificates .....                       | <a href="#">1188</a>                        | ESXi host .....                                       | <a href="#">1337</a>    |
| removing users from role .....                            | <a href="#">193</a> , <a href="#">254</a>   | restore .....                                         | <a href="#">838</a>     |
| removing vCenter .....                                    | <a href="#">1380</a>                        | primary System Manager .....                          | <a href="#">115</a>     |
| renewing identity certificates .....                      | <a href="#">1194</a>                        | primary System Manager server .....                   | <a href="#">127–129</a> |
| repairing a replica node .....                            | <a href="#">1073</a>                        | Restore                                               |                         |
| replace                                                   |                                             | field descriptions .....                              | <a href="#">856</a>     |
| primary System Manager server .....                       | <a href="#">126</a>                         | restore backup                                        |                         |
| secondary System Manager server .....                     | <a href="#">128</a>                         | remote server .....                                   | <a href="#">848</a>     |
| replace identity certificates                             |                                             | restore backup from remote server .....               | <a href="#">848</a>     |
| field descriptions .....                                  | <a href="#">1195</a>                        | Restore Confirmation Page .....                       | <a href="#">368</a>     |
| replace primary System Manager server using secondary     |                                             | restore data backup .....                             | <a href="#">847</a>     |
| System Manager .....                                      | <a href="#">128</a>                         | restore on System Manager Geographic Redundancy ..... | <a href="#">840</a>     |
| replace System Manager servers .....                      | <a href="#">126</a>                         | restore system backup from local server .....         | <a href="#">847</a>     |
| replacing identity certificates .....                     | <a href="#">1192</a>                        | restoring                                             |                         |
| replica group                                             |                                             | default password policy settings .....                | <a href="#">69</a>      |
| remove nodes .....                                        | <a href="#">1074</a>                        | restoring, deleted user .....                         | <a href="#">253</a>     |
| replica groups; view .....                                | <a href="#">1072</a>                        | restoring all announcements .....                     | <a href="#">675</a>     |
| Replica Groups page .....                                 | <a href="#">1075</a>                        | restoring announcements .....                         | <a href="#">675</a>     |
| replication                                               |                                             | restoring announcements; all .....                    | <a href="#">675</a>     |
| database .....                                            | <a href="#">100</a>                         | restoring audio groups .....                          | <a href="#">684</a>     |
| file .....                                                | <a href="#">100</a>                         | restoring audio groups; field description .....       | <a href="#">684</a>     |
| LDAP .....                                                | <a href="#">100</a>                         | restoring the backup data through CLI .....           | <a href="#">849</a>     |
| report .....                                              | <a href="#">1088</a>                        | Restoring the default password policy settings .....  | <a href="#">69</a>      |
| Report alarm properties .....                             | <a href="#">869</a>                         | restoring through command line .....                  | <a href="#">849</a>     |
| reports .....                                             | <a href="#">1082</a> , <a href="#">1089</a> | Restrict Last Appearance .....                        | <a href="#">753</a>     |
| delete .....                                              | <a href="#">1092</a>                        | retrieve harvested log file .....                     | <a href="#">1004</a>    |
| download .....                                            | <a href="#">1090</a>                        | retrieving                                            |                         |
| email .....                                               | <a href="#">1092</a>                        | local WebLM certificate .....                         | <a href="#">1047</a>    |
| generate .....                                            | <a href="#">1089</a>                        | retrieving the System Manager CA certificate .....    | <a href="#">1209</a>    |
| generating .....                                          | <a href="#">1085</a>                        | retrying                                              |                         |
| new .....                                                 | <a href="#">1089</a>                        | Utility Services to AVP Utilities upgrade .....       | <a href="#">1322</a>    |
| rerun .....                                               | <a href="#">1088</a>                        | revocation information .....                          | <a href="#">1227</a>    |
| Reports Generation field descriptions .....               | <a href="#">1083</a>                        | revocation in SubCA .....                             | <a href="#">1227</a>    |
| Reports output directory .....                            | <a href="#">869</a>                         | revoke certificate field descriptions .....           | <a href="#">1199</a>    |

|                                                           |                                      |                                                        |                               |
|-----------------------------------------------------------|--------------------------------------|--------------------------------------------------------|-------------------------------|
| revoking certificates .....                               | <a href="#">1199</a>                 | saving an endpoint template .....                      | <a href="#">715</a>           |
| Rng .....                                                 | <a href="#">705</a>                  | saving announcements .....                             | <a href="#">673</a>           |
| role                                                      |                                      | saving CM translations .....                           | <a href="#">978</a>           |
| add .....                                                 | <a href="#">195</a>                  | saving Communication Manager translations .....        | <a href="#">978</a>           |
| assign users .....                                        | <a href="#">192</a>                  | schedule                                               |                               |
| copy permission mapping .....                             | <a href="#">193</a>                  | on-demand job .....                                    | <a href="#">1096</a>          |
| delete .....                                              | <a href="#">194</a>                  | schedule a user import job .....                       | <a href="#">397</a>           |
| details .....                                             | <a href="#">196</a>                  | Schedule Backup page .....                             | <a href="#">855</a>           |
| edit .....                                                | <a href="#">194</a>                  | schedule CRL download                                  |                               |
| new .....                                                 | <a href="#">195</a>                  | field descriptions .....                               | <a href="#">1234</a>          |
| unassign users .....                                      | <a href="#">193, 254</a>             | schedule CRL download field descriptions .....         | <a href="#">1234</a>          |
| role based access control .....                           | <a href="#">181</a>                  | schedule data backup; remote server .....              | <a href="#">844</a>           |
| Role Details .....                                        | <a href="#">196</a>                  | scheduled backup job                                   |                               |
| Role page .....                                           | <a href="#">194</a>                  | deleting .....                                         | <a href="#">846</a>           |
| roles                                                     |                                      | Schedule Discovery .....                               | <a href="#">901</a>           |
| built-in .....                                            | <a href="#">182</a>                  | scheduled job                                          |                               |
| RBAC .....                                                | <a href="#">186</a>                  | edit .....                                             | <a href="#">1108</a>          |
| remove .....                                              | <a href="#">251</a>                  | scheduled jobs                                         |                               |
| Service Provider Administrator .....                      | <a href="#">182</a>                  | completed .....                                        | <a href="#">1105</a>          |
| System Administrator .....                                | <a href="#">182</a>                  | scheduler .....                                        | <a href="#">1096</a>          |
| Tenant Administrator .....                                | <a href="#">182</a>                  | Scheduler                                              |                               |
| Roles .....                                               | <a href="#">181</a>                  | permissions .....                                      | <a href="#">1097</a>          |
| rolling back                                              |                                      | scheduler; access .....                                | <a href="#">1097</a>          |
| Utility Services .....                                    | <a href="#">1322</a>                 | scheduler service .....                                | <a href="#">1096</a>          |
| Room                                                      |                                      | scheduling                                             |                               |
| Station .....                                             | <a href="#">754</a>                  | CRL download .....                                     | <a href="#">1234</a>          |
| root CA .....                                             | <a href="#">1231</a>                 | scheduling a data backup on a local server .....       | <a href="#">844</a>           |
| root CA created using SHA256withRSA signing algorithm and |                                      | scheduling a data backup on a remote server .....      | <a href="#">844</a>           |
| 2048 key size .....                                       | <a href="#">1215</a>                 | scheduling a global user settings import job .....     | <a href="#">404</a>           |
| route pattern                                             |                                      | scheduling a user synchronization job .....            | <a href="#">92</a>            |
| calculate .....                                           | <a href="#">832</a>                  | SCP Configuration (S) .....                            | <a href="#">1305</a>          |
| route selection .....                                     | <a href="#">832</a>                  | SDM                                                    |                               |
| rules .....                                               | <a href="#">613</a>                  | installation .....                                     | <a href="#">1280</a>          |
| runRTSCli.sh .....                                        | <a href="#">917, 918</a>             | SDM Client .....                                       | <a href="#">1277</a>          |
|                                                           |                                      | SDM elements                                           |                               |
|                                                           |                                      | re-establishing trust .....                            | <a href="#">1356</a>          |
| <b>S</b>                                                  |                                      | search                                                 |                               |
| SAC/CF Override .....                                     | <a href="#">756</a>                  | Communication Manager objects .....                    | <a href="#">650</a>           |
| Salient features of SAML implementation in System Manager |                                      | Search Archives page .....                             | <a href="#">1015</a>          |
| .....                                                     | <a href="#">1247</a>                 | searching                                              |                               |
| SAML .....                                                | <a href="#">1246</a>                 | 96x1 SIP set type for J1xx endpoint migration by using |                               |
| SAML authentication .....                                 | <a href="#">1245</a>                 | advanced search .....                                  | <a href="#">727</a>           |
| SAML implementation .....                                 | <a href="#">1246, 1247</a>           | search component .....                                 | <a href="#">249</a>           |
| SAML protocol .....                                       | <a href="#">1245</a>                 | users .....                                            | <a href="#">249</a>           |
| SAMP/MPC firmware                                         |                                      | searching Communication Manager objects .....          | <a href="#">650</a>           |
| update .....                                              | <a href="#">1486</a>                 | searching contacts on Avaya SIP AST endpoints .....    | <a href="#">1263</a>          |
| SAMP firmware                                             |                                      | searching for alarms .....                             | <a href="#">993</a>           |
| update .....                                              | <a href="#">1486</a>                 | searching for a text in a log file .....               | <a href="#">1008</a>          |
| sample scenario                                           |                                      | searching for content .....                            | <a href="#">1535</a>          |
| range feature .....                                       | <a href="#">202</a>                  | searching for logs .....                               | <a href="#">1024</a>          |
| sample upgrade scenario .....                             | <a href="#">1455–1457, 1474–1476</a> | searching for resources .....                          | <a href="#">164, 165, 177</a> |
| sample upgrade workflow .....                             | <a href="#">1455–1457, 1474–1476</a> | searching logs .....                                   | <a href="#">1024</a>          |
| sample XML file for a user with SIP Communication Profile |                                      | search resource .....                                  | <a href="#">178</a>           |
| .....                                                     | <a href="#">592</a>                  | search users .....                                     | <a href="#">249</a>           |
| sample XML with a single user profile .....               | <a href="#">588</a>                  | secondary alarms                                       |                               |
| Save as template .....                                    | <a href="#">715</a>                  | forward to primary System Manager .....                | <a href="#">996</a>           |
| saving an announcement .....                              | <a href="#">673</a>                  | secondary server .....                                 | <a href="#">113</a>           |



|                                                                                  |                                           |                                                          |                                                                    |
|----------------------------------------------------------------------------------|-------------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------|
| secondary server ( <i>continued</i> )                                            |                                           | Service Link Mode                                        |                                                                    |
| CRL addition .....                                                               | <a href="#">107</a>                       | Attendant Console .....                                  | <a href="#">744</a>                                                |
| secondary server alarms                                                          |                                           | service observe                                          |                                                                    |
| view .....                                                                       | <a href="#">997</a>                       | coach .....                                              | <a href="#">775</a>                                                |
| secondary Session Manager .....                                                  | <a href="#">739</a>                       | listen-only .....                                        | <a href="#">775</a>                                                |
| secondary System Manager                                                         |                                           | Service Profile Management .....                         | <a href="#">864</a>                                                |
| modify FQDN .....                                                                | <a href="#">1515</a>                      | Services Port static route update .....                  | <a href="#">1360</a>                                               |
| modify IP address .....                                                          | <a href="#">1515</a>                      | Session Manager                                          |                                                                    |
| secondary System Manager failure .....                                           | <a href="#">128</a>                       | configure during GR failover .....                       | <a href="#">134</a>                                                |
| Security Code .....                                                              | <a href="#">738</a>                       | Session Manager communication profile administration ... | <a href="#">260</a>                                                |
| security configuration                                                           |                                           | Session Manager Communication profile administration ... | <a href="#">261</a>                                                |
| field descriptions .....                                                         | <a href="#">1237</a>                      | Session Manager configuration .....                      | <a href="#">133</a>                                                |
| security configuration field descriptions .....                                  | <a href="#">1237</a>                      | Session Manager correlation .....                        | <a href="#">836</a>                                                |
| security hardening .....                                                         | <a href="#">1166</a>                      | Session Manager update .....                             | <a href="#">1357</a> , <a href="#">1397</a> , <a href="#">1399</a> |
| commercial grade .....                                                           | <a href="#">1163</a>                      | session properties; edit .....                           | <a href="#">71</a>                                                 |
| military grade .....                                                             | <a href="#">1164</a>                      | session properties field descriptions .....              | <a href="#">71</a>                                                 |
| System Manager .....                                                             | <a href="#">1162</a>                      | Session termination policy .....                         | <a href="#">71</a>                                                 |
| security settings .....                                                          | <a href="#">72</a>                        | Set Color .....                                          | <a href="#">754</a>                                                |
| field descriptions .....                                                         | <a href="#">73</a>                        | set enrollment password .....                            | <a href="#">1181</a>                                               |
| select all attribute; edit .....                                                 | <a href="#">650</a>                       | setting .....                                            | <a href="#">756</a>                                                |
| selected groups; adding resources .....                                          | <a href="#">176</a>                       | Settings icon .....                                      | <a href="#">46</a>                                                 |
| Selected Roles .....                                                             | <a href="#">365</a> , <a href="#">369</a> | setting the default CA .....                             | <a href="#">1229</a>                                               |
| Select Flexi Footprint .....                                                     | <a href="#">1358</a>                      | setting the new CA as default CA .....                   | <a href="#">1229</a>                                               |
| Select Last Used Appearance .....                                                | <a href="#">751</a>                       | set type .....                                           | <a href="#">773</a>                                                |
| select upgrade target release .....                                              | <a href="#">1396</a>                      | H323 .....                                               | <a href="#">777</a>                                                |
| Select Users .....                                                               | <a href="#">369</a>                       | set type of endpoints .....                              | <a href="#">773</a>                                                |
| self provisioning                                                                |                                           | set up alternate source .....                            | <a href="#">1288</a>                                               |
| disable .....                                                                    | <a href="#">221</a>                       | SFTP Configuration (T) .....                             | <a href="#">1305</a>                                               |
| enable .....                                                                     | <a href="#">221</a>                       | SHA256withRSA signing algorithm and 2048 key size ...    | <a href="#">1216</a>                                               |
| end user .....                                                                   | <a href="#">221</a> , <a href="#">223</a> | SHA2 signing algorithm and 2048 key size .....           | <a href="#">1216</a>                                               |
| Sending reports through email .....                                              | <a href="#">1092</a>                      | shared address .....                                     | <a href="#">604</a> , <a href="#">607</a>                          |
| Server Host ID .....                                                             | <a href="#">1045</a>                      | assigning .....                                          | <a href="#">255</a> , <a href="#">604</a>                          |
| Server Properties .....                                                          | <a href="#">1045</a>                      | shared addresses .....                                   | <a href="#">219</a>                                                |
| server properties; view .....                                                    | <a href="#">1036</a>                      | sharing content .....                                    | <a href="#">1535</a>                                               |
| server support                                                                   |                                           | shutdown .....                                           | <a href="#">1272</a>                                               |
| Communication Manager 5.2.1 upgrade .....                                        | <a href="#">1476</a>                      | shut down from web console .....                         | <a href="#">1273</a>                                               |
| Server support                                                                   |                                           | shut down System Manager .....                           | <a href="#">1273</a>                                               |
| Communication Manager 5.2.1 to 6.3.100 .....                                     | <a href="#">1476</a>                      | shutting down                                            |                                                                    |
| Server support for Communication Manager Release 5.2.1 to 6.3.100 upgrades ..... | <a href="#">1476</a>                      | AVP .....                                                | <a href="#">1337</a>                                               |
| service                                                                          |                                           | signing the certificate .....                            | <a href="#">1224</a>                                               |
| Health Monitor .....                                                             | <a href="#">119</a>                       | simultaneous logins .....                                | <a href="#">988</a>                                                |
| serviceability agent                                                             |                                           | Single administration                                    |                                                                    |
| activate .....                                                                   | <a href="#">968</a>                       | Dual Registration .....                                  | <a href="#">777</a>                                                |
| assign filter profile .....                                                      | <a href="#">964</a>                       | Single Sign-On .....                                     | <a href="#">1245</a> – <a href="#">1247</a>                        |
| unassign filter profile .....                                                    | <a href="#">965</a>                       | single sign-on cookie domain .....                       | <a href="#">75</a>                                                 |
| serviceability agents .....                                                      | <a href="#">954</a>                       | Single Sign On to remote machine fails .....             | <a href="#">1509</a>                                               |
| activate .....                                                                   | <a href="#">967</a>                       | SIP endpoint                                             |                                                                    |
| Serviceability agents                                                            |                                           | feature button .....                                     | <a href="#">773</a>                                                |
| Manage Profile Job Status .....                                                  | <a href="#">969</a>                       | SIP endpoints .....                                      | <a href="#">778</a>                                                |
| repair .....                                                                     | <a href="#">967</a>                       | site                                                     |                                                                    |
| Service Hours Table                                                              |                                           | create .....                                             | <a href="#">1256</a>                                               |
| downloading excel template .....                                                 | <a href="#">697</a>                       | editing .....                                            | <a href="#">1261</a>                                               |
| exporting all service hours table .....                                          | <a href="#">696</a>                       | viewing .....                                            | <a href="#">1260</a>                                               |
| exporting selected service hours table .....                                     | <a href="#">696</a>                       | Site Data .....                                          | <a href="#">754</a>                                                |
| importing service hours table .....                                              | <a href="#">696</a>                       | building .....                                           | <a href="#">754</a>                                                |
| Service Hours Table List .....                                                   | <a href="#">695</a>                       | cable .....                                              | <a href="#">754</a>                                                |
|                                                                                  |                                           | floor .....                                              | <a href="#">754</a>                                                |

|                                               |                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Site Data ( <i>continued</i> )                |                                                                                                                  |
| jack                                          | <a href="#">754</a>                                                                                              |
| room                                          | <a href="#">754</a>                                                                                              |
| SMGR_DEFAULT_LOCAL                            | <a href="#">1294</a>                                                                                             |
| Snapshot Manager                              |                                                                                                                  |
| virtual machine snapshot                      | <a href="#">1342</a>                                                                                             |
| Snapshot Manager field descriptions           | <a href="#">1343</a>                                                                                             |
| SNMP access profile                           |                                                                                                                  |
| edit                                          | <a href="#">904</a>                                                                                              |
| SNMP Access profile                           |                                                                                                                  |
| add                                           | <a href="#">904</a>                                                                                              |
| delete                                        | <a href="#">905</a>                                                                                              |
| SNMP Access Profile                           | <a href="#">906</a>                                                                                              |
| SNMP Access Profiles                          | <a href="#">905</a>                                                                                              |
| SNMP alarms                                   |                                                                                                                  |
| CS 1000                                       | <a href="#">139</a>                                                                                              |
| SNMP attributes                               | <a href="#">936</a>                                                                                              |
| SNMP discovery                                |                                                                                                                  |
| device list                                   | <a href="#">901</a>                                                                                              |
| SNMP target profile                           |                                                                                                                  |
| add                                           | <a href="#">960</a>                                                                                              |
| edit                                          | <a href="#">961</a>                                                                                              |
| SNMP target profile; view                     | <a href="#">960</a>                                                                                              |
| SNMP target profile list                      | <a href="#">959</a>                                                                                              |
| SNMP target profiles; delete                  | <a href="#">961</a>                                                                                              |
| SNMP target profiles field descriptions       | <a href="#">962</a>                                                                                              |
| SNMP traps                                    | <a href="#">1030</a>                                                                                             |
| SNMP V1                                       | <a href="#">906</a>                                                                                              |
| SNMP V1 protocol                              | <a href="#">905</a>                                                                                              |
| SNMP V3                                       | <a href="#">906</a>                                                                                              |
| SNMP V3 protocol                              | <a href="#">905</a>                                                                                              |
| SNMPv3 user profile; add                      | <a href="#">956</a>                                                                                              |
| SNMPv3 user profile; create                   | <a href="#">956</a>                                                                                              |
| SNMPv3 user profile; delete                   | <a href="#">957</a>                                                                                              |
| SNMPv3 user profile; edit                     | <a href="#">957</a>                                                                                              |
| SNMPv3 user profile; filter                   | <a href="#">958</a>                                                                                              |
| SNMPv3 user profile; view                     | <a href="#">957</a>                                                                                              |
| SNMPv3 user profiles                          |                                                                                                                  |
| assign                                        | <a href="#">969</a>                                                                                              |
| manage                                        | <a href="#">969</a>                                                                                              |
| SNMPv3 user profiles field description        | <a href="#">958</a>                                                                                              |
| software                                      |                                                                                                                  |
| analyze                                       | <a href="#">1444</a>                                                                                             |
| download                                      | <a href="#">1307</a> , <a href="#">1312</a> , <a href="#">1445</a>                                               |
| Software inventory                            |                                                                                                                  |
| field descriptions                            | <a href="#">1460</a>                                                                                             |
| Software Inventory                            | <a href="#">1439</a>                                                                                             |
| Software Inventory field descriptions         | <a href="#">1460</a>                                                                                             |
| software library                              |                                                                                                                  |
| delete                                        | <a href="#">1304</a> , <a href="#">1309</a>                                                                      |
| protocol support                              | <a href="#">1294</a>                                                                                             |
| software library management                   | <a href="#">1308</a>                                                                                             |
| sync files                                    | <a href="#">1309</a>                                                                                             |
| upload files                                  | <a href="#">1309</a>                                                                                             |
| viewing a file                                | <a href="#">1308</a>                                                                                             |
| Software library                              | <a href="#">1292</a>                                                                                             |
| software library; add                         | <a href="#">1303</a>                                                                                             |
| software library; create                      | <a href="#">1303</a>                                                                                             |
| software library; edit                        | <a href="#">1304</a>                                                                                             |
| software library; view                        | <a href="#">1304</a>                                                                                             |
| software library; viewing files               | <a href="#">1307</a>                                                                                             |
| software library files                        | <a href="#">1309</a>                                                                                             |
| software library files field descriptions     | <a href="#">1309</a>                                                                                             |
| software management                           |                                                                                                                  |
| analyze software                              | <a href="#">1445</a>                                                                                             |
| Software Management                           | <a href="#">1392</a>                                                                                             |
| Solution Deployment Manager                   | <a href="#">1276</a> , <a href="#">1311</a> , <a href="#">1328</a> , <a href="#">1355</a> , <a href="#">1392</a> |
| permissions                                   | <a href="#">190</a>                                                                                              |
| restart application                           | <a href="#">1361</a>                                                                                             |
| start application                             | <a href="#">1360</a>                                                                                             |
| stop application                              | <a href="#">1361</a>                                                                                             |
| supported applications                        | <a href="#">1285</a>                                                                                             |
| Solution Deployment Manager client            | <a href="#">1276</a>                                                                                             |
| Solution Deployment Manager Client            | <a href="#">1277</a>                                                                                             |
| prerequisites                                 | <a href="#">1279</a>                                                                                             |
| Solution Deployment Manager client dashboard  | <a href="#">1283</a>                                                                                             |
| Solution Deployment Manager elements          |                                                                                                                  |
| re-establishing trust                         | <a href="#">1356</a>                                                                                             |
| sort documents by last updated                | <a href="#">1535</a>                                                                                             |
| Speaker                                       | <a href="#">755</a>                                                                                              |
| Speakerphone                                  | <a href="#">745</a>                                                                                              |
| specifying range for endpoints                | <a href="#">209</a>                                                                                              |
| specifying range for hunt group               | <a href="#">213</a>                                                                                              |
| SSH from AVP Utilities                        | <a href="#">1332</a>                                                                                             |
| SSO configuration                             |                                                                                                                  |
| Avaya Equinox Management                      | <a href="#">153</a>                                                                                              |
| SSO cookie domain value                       | <a href="#">1509</a>                                                                                             |
| reimport                                      | <a href="#">75</a>                                                                                               |
| SSO for Conferencing                          | <a href="#">150</a>                                                                                              |
| SSO login                                     | <a href="#">1509</a>                                                                                             |
| stand-alone                                   | <a href="#">119</a>                                                                                              |
| start                                         |                                                                                                                  |
| application                                   | <a href="#">1360</a>                                                                                             |
| start application from SDM                    | <a href="#">1360</a>                                                                                             |
| static routing                                |                                                                                                                  |
| changing                                      | <a href="#">1360</a>                                                                                             |
| updating                                      | <a href="#">1360</a>                                                                                             |
| status                                        |                                                                                                                  |
| Analyze                                       | <a href="#">1438</a>                                                                                             |
| analyze job                                   | <a href="#">1436</a>                                                                                             |
| element records import                        | <a href="#">946</a>                                                                                              |
| Preupgrade check                              | <a href="#">1438</a>                                                                                             |
| preupgrade check job                          | <a href="#">1436</a>                                                                                             |
| Refresh elements job                          | <a href="#">1436</a>                                                                                             |
| upgrade job                                   | <a href="#">1436</a>                                                                                             |
| upgrade jobs                                  | <a href="#">1438</a>                                                                                             |
| stop                                          |                                                                                                                  |
| application                                   | <a href="#">1361</a>                                                                                             |
| stop application from SDM                     | <a href="#">1361</a>                                                                                             |
| Stop Confirmation page                        | <a href="#">1111</a>                                                                                             |
| stopping pending jobs                         | <a href="#">1102</a>                                                                                             |
| submitting a request for harvesting log files | <a href="#">1007</a>                                                                                             |
| Subnet Configurations field descriptions      | <a href="#">909</a>                                                                                              |
| subnets                                       | <a href="#">909</a>                                                                                              |

|                                                             |                                             |                                                                |                                         |
|-------------------------------------------------------------|---------------------------------------------|----------------------------------------------------------------|-----------------------------------------|
| subnets list .....                                          | <a href="#">909</a>                         | synchronization datasource ( <i>continued</i> ) .....          |                                         |
| subnetwork .....                                            |                                             | deleting .....                                                 | <a href="#">85</a>                      |
| add .....                                                   | <a href="#">908</a>                         | edit .....                                                     | <a href="#">84</a>                      |
| delete .....                                                | <a href="#">909</a>                         | synchronization from LDAP directory server .....               | <a href="#">81</a> , <a href="#">82</a> |
| edit .....                                                  | <a href="#">908</a>                         | synchronization job history .....                              | <a href="#">93</a>                      |
| subordinate CA .....                                        | <a href="#">1227</a> , <a href="#">1231</a> | synchronization job history field description .....            | <a href="#">94</a>                      |
| subscriber .....                                            |                                             | synchronization job summary .....                              |                                         |
| adding templates .....                                      | <a href="#">1121</a>                        | view .....                                                     | <a href="#">94</a>                      |
| subscriber; view .....                                      |                                             | synchronization notification .....                             | <a href="#">1497</a>                    |
| viewing subscribers .....                                   | <a href="#">641</a>                         | synchronization to LDAP directory server .....                 | <a href="#">81</a>                      |
| subscriber class of service .....                           | <a href="#">639</a>                         | synchronize .....                                              |                                         |
| subscriber COS .....                                        | <a href="#">639</a>                         | CM data .....                                                  | <a href="#">974</a>                     |
| subscriber list .....                                       | <a href="#">642</a>                         | configuring options .....                                      | <a href="#">974</a>                     |
| Subscriber Manager .....                                    |                                             | CS 1000 profile .....                                          | <a href="#">983</a>                     |
| datasource attributes .....                                 | <a href="#">633</a>                         | synchronize CM data .....                                      | <a href="#">974</a>                     |
| datasource parameters .....                                 | <a href="#">633</a>                         | synchronize communication profiles field description .....     | <a href="#">983</a>                     |
| Subscriber Manager data .....                               |                                             | synchronize UCM and Application Server system .....            |                                         |
| import .....                                                | <a href="#">631</a>                         | configuration .....                                            | <a href="#">977</a>                     |
| Subscriber Manager user data .....                          |                                             | synchronizing .....                                            |                                         |
| importing .....                                             | <a href="#">636</a>                         | Communication Manager data .....                               | <a href="#">972</a>                     |
| subscribers .....                                           |                                             | IP Office .....                                                | <a href="#">972</a>                     |
| delete .....                                                | <a href="#">641</a>                         | Messaging data .....                                           | <a href="#">972</a>                     |
| deleting .....                                              | <a href="#">641</a>                         | synchronizing communication profiles .....                     | <a href="#">981</a>                     |
| removing .....                                              | <a href="#">641</a>                         | synchronizing CS 1000 profiles .....                           | <a href="#">981</a>                     |
| subscribers; add .....                                      |                                             | synchronizing messaging data .....                             | <a href="#">978</a>                     |
| adding subscribers .....                                    | <a href="#">640</a>                         | synchronizing resources .....                                  | <a href="#">163</a>                     |
| subscribers; new .....                                      | <a href="#">640</a>                         | synchronizing System Manager master database and replica ..... | <a href="#">1073</a>                    |
| subscribers; edit .....                                     |                                             | computer database .....                                        | <a href="#">1073</a>                    |
| editing a subscriber .....                                  | <a href="#">641</a>                         | Synchronizing the VMPro system configuration .....             | <a href="#">977</a>                     |
| editing subscribers .....                                   | <a href="#">641</a>                         | syslog messages .....                                          |                                         |
| subscriber template list .....                              | <a href="#">1124</a>                        | forwarding to remote server .....                              | <a href="#">1019</a>                    |
| subscriber templates .....                                  |                                             | syslog receiver configuration .....                            |                                         |
| delete .....                                                | <a href="#">1123</a>                        | field descriptions .....                                       | <a href="#">1384</a>                    |
| duplicate .....                                             | <a href="#">1123</a>                        | syslog server .....                                            |                                         |
| edit .....                                                  | <a href="#">1122</a>                        | adding .....                                                   | <a href="#">1383</a>                    |
| view .....                                                  | <a href="#">1123</a>                        | configuration .....                                            | <a href="#">1383</a>                    |
| subscriber template versions .....                          | <a href="#">1114</a>                        | system .....                                                   |                                         |
| support .....                                               | <a href="#">1537</a>                        | scheduled job .....                                            | <a href="#">1096</a>                    |
| Supported servers .....                                     | <a href="#">1450</a>                        | System ID .....                                                | <a href="#">739</a>                     |
| support of common parameters across endpoint template ..... | <a href="#">765</a>                         | System Manager .....                                           | <a href="#">1231</a>                    |
| Survivable COR .....                                        | <a href="#">745</a>                         | 7.0 .....                                                      | <a href="#">1437</a>                    |
| Survivable GK Node Name .....                               | <a href="#">746</a>                         | commands .....                                                 | <a href="#">1518</a>                    |
| Survivable Trunk Dest .....                                 | <a href="#">751</a>                         | disabling FTP .....                                            | <a href="#">1293</a>                    |
| svars .....                                                 |                                             | enabling FTP .....                                             | <a href="#">1293</a>                    |
| file size .....                                             | <a href="#">839</a>                         | local software library .....                                   | <a href="#">1294</a>                    |
| swap endpoints field descriptions .....                     | <a href="#">770</a>                         | new in release 8.1.1 .....                                     | <a href="#">41</a>                      |
| symmetric keys .....                                        |                                             | new in release 8.1.2 .....                                     | <a href="#">41</a>                      |
| regenerating .....                                          | <a href="#">1251</a>                        | new in release 8.1.3 .....                                     | <a href="#">39</a>                      |
| sync .....                                                  | <a href="#">835</a>                         | new in release 8.1.3.1 .....                                   | <a href="#">38</a>                      |
| Sync files .....                                            | <a href="#">1309</a>                        | upgrade .....                                                  | <a href="#">1437</a>                    |
| synchronization .....                                       | <a href="#">80</a> , <a href="#">1071</a>   | System Manager; Communication Manager capabilities .....       | <a href="#">648</a>                     |
| DRS clients .....                                           | <a href="#">1071</a>                        | System Manager; firewall .....                                 | <a href="#">1539</a>                    |
| incremental .....                                           | <a href="#">972</a>                         | System Manager; firewall implementation .....                  | <a href="#">1539</a>                    |
| initialization .....                                        | <a href="#">972</a>                         | System Manager 8.1 .....                                       |                                         |
| limitations .....                                           | <a href="#">82</a>                          | new in release .....                                           | <a href="#">42</a>                      |
| synchronization datasource .....                            |                                             | System Manager Application Management .....                    |                                         |
| add .....                                                   | <a href="#">82</a>                          | Installed Patches field descriptions .....                     | <a href="#">1373</a>                    |

|                                                         |                          |                                                          |                            |
|---------------------------------------------------------|--------------------------|----------------------------------------------------------|----------------------------|
| System Manager CA as subordinate CA .....               | <a href="#">1224</a>     | tenant ( <i>continued</i> ) .....                        |                            |
| System Manager CA certificate; retrieve .....           | <a href="#">1209</a>     | viewing .....                                            | <a href="#">1260</a>       |
| System Manager capabilities .....                       |                          | tenant administrator .....                               |                            |
| certificate generation .....                            | <a href="#">1178</a>     | assign .....                                             | <a href="#">1259</a>       |
| certificate management .....                            | <a href="#">1178</a>     | unassign .....                                           | <a href="#">1260</a>       |
| System Manager certificate authority .....              | <a href="#">1224</a>     | tenant administrator role .....                          |                            |
| System Manager dashboard .....                          | <a href="#">46, 49</a>   | add .....                                                | <a href="#">189</a>        |
| System Manager localization .....                       | <a href="#">1531</a>     | tenant management .....                                  | <a href="#">1259, 1260</a> |
| System Manager login .....                              | <a href="#">49</a>       | Tenant Management .....                                  | <a href="#">1254</a>       |
| System Manager logon messages .....                     | <a href="#">51</a>       | console .....                                            | <a href="#">57</a>         |
| System Manager messages .....                           | <a href="#">50</a>       | field descriptions .....                                 | <a href="#">1267</a>       |
| System Manager restore .....                            | <a href="#">115</a>      | Tenant Management page .....                             | <a href="#">1267</a>       |
| System Manager server for upgrade .....                 | <a href="#">1292</a>     | tenant organization .....                                |                            |
| System Manager shutdown .....                           | <a href="#">1272</a>     | create .....                                             | <a href="#">1256</a>       |
| System Manager training .....                           | <a href="#">1536</a>     | tenant partitioning .....                                |                            |
| System Manager trust store; Communication Manager ..... |                          | Avaya SIP AST endpoints .....                            | <a href="#">1263</a>       |
| certificate .....                                       | <a href="#">1503</a>     | Communication Manager .....                              | <a href="#">1263</a>       |
| System Manager upgrade .....                            | <a href="#">1428</a>     | Terminate to Coverage Pts. with Bridged Appearances .... | <a href="#">705</a>        |
| System Manager VM update .....                          | <a href="#">1374</a>     | Terminating .....                                        |                            |
| System Manager web console .....                        | <a href="#">46</a>       | administrative user sessions .....                       | <a href="#">78</a>         |
| System Platform .....                                   |                          | terminating single sign-on sessions .....                | <a href="#">1250</a>       |
| add .....                                               | <a href="#">923</a>      | test alarm from CLI .....                                |                            |
| System Platform upgrades .....                          |                          | generate .....                                           | <a href="#">996</a>        |
| preupgrade checks .....                                 | <a href="#">1449</a>     | test alarms from web console .....                       |                            |
| system recovery process .....                           | <a href="#">129</a>      | generate .....                                           | <a href="#">995</a>        |
| system requirements for the external server .....       | <a href="#">1310</a>     | third-party AVP certificates .....                       |                            |
| system template .....                                   |                          | creating generic CSR .....                               | <a href="#">1211, 1341</a> |
| manage audio field description .....                    | <a href="#">1149</a>     | editing generic CSR .....                                | <a href="#">1211, 1341</a> |
| <b>T</b>                                                |                          |                                                          |                            |
| target profile; manage .....                            | <a href="#">968</a>      | third-party certificates .....                           |                            |
| target profiles .....                                   | <a href="#">954</a>      | applying to Appliance Virtualization Platform ..         | <a href="#">1210, 1339</a> |
| edit .....                                              | <a href="#">961</a>      | third-party identity certificate .....                   | <a href="#">1223</a>       |
| target profiles; delete .....                           | <a href="#">961</a>      | threshold value .....                                    |                            |
| target profiles; filter .....                           | <a href="#">960</a>      | disk space .....                                         | <a href="#">840</a>        |
| target profiles field descriptions .....                | <a href="#">962</a>      | throttling period .....                                  | <a href="#">994</a>        |
| target release .....                                    | <a href="#">1396</a>     | Through .....                                            | <a href="#">779</a>        |
| select .....                                            | <a href="#">1396</a>     | Time of Day Coverage Table .....                         | <a href="#">708</a>        |
| team .....                                              |                          | Time of Day Lock Table .....                             | <a href="#">746</a>        |
| create .....                                            | <a href="#">1256</a>     | timeout interval .....                                   |                            |
| editing .....                                           | <a href="#">1261</a>     | configure .....                                          | <a href="#">120</a>        |
| viewing .....                                           | <a href="#">1260</a>     | time zone .....                                          |                            |
| template .....                                          | <a href="#">1450</a>     | configure .....                                          | <a href="#">1530</a>       |
| map permissions .....                                   | <a href="#">191</a>      | TN .....                                                 | <a href="#">737</a>        |
| Template for permission set .....                       | <a href="#">191, 197</a> | TN boards .....                                          |                            |
| template list .....                                     | <a href="#">1124</a>     | upgrade .....                                            | <a href="#">1478</a>       |
| templates .....                                         | <a href="#">1114</a>     | TN Boards .....                                          |                            |
| new subscriber .....                                    | <a href="#">1121</a>     | protocols .....                                          | <a href="#">1486</a>       |
| upgrade .....                                           | <a href="#">1115</a>     | TrapListener .....                                       | <a href="#">1030</a>       |
| templates for mapping permission .....                  | <a href="#">191</a>      | TrapListener service .....                               | <a href="#">1030</a>       |
| template versioning .....                               | <a href="#">1114</a>     | Traplistener service; alarming UI .....                  | <a href="#">889</a>        |
| template versions .....                                 | <a href="#">1114</a>     | TrapListener service; configure .....                    | <a href="#">889</a>        |
| tenant .....                                            |                          | Triple Ringer Type .....                                 |                            |
| create .....                                            | <a href="#">1256</a>     | Call Pickup button .....                                 | <a href="#">774</a>        |
| delete .....                                            | <a href="#">1261</a>     | configuration .....                                      | <a href="#">774</a>        |
| editing .....                                           | <a href="#">1261</a>     | trunk group .....                                        |                            |
|                                                         |                          | adding .....                                             | <a href="#">784</a>        |
|                                                         |                          | delete .....                                             | <a href="#">786</a>        |
|                                                         |                          | editing .....                                            | <a href="#">785</a>        |

|                                                            |                                                                                           |  |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------|--|
| trunk group ( <i>continued</i> )                           |                                                                                           |  |
| field-level RBAC .....                                     | <a href="#">217</a>                                                                       |  |
| viewing .....                                              | <a href="#">785</a>                                                                       |  |
| Trunk Group List                                           |                                                                                           |  |
| field descriptions .....                                   | <a href="#">784</a>                                                                       |  |
| trusted certificate .....                                  | <a href="#">1189</a>                                                                      |  |
| trusted certificate; add .....                             | <a href="#">1500</a>                                                                      |  |
| trusted certificates                                       |                                                                                           |  |
| add .....                                                  | <a href="#">1184</a>                                                                      |  |
| view .....                                                 | <a href="#">1187</a>                                                                      |  |
| trusted certificates; remove .....                         | <a href="#">1188</a>                                                                      |  |
| Trust Management .....                                     | <a href="#">1178</a>                                                                      |  |
| Trust management for Conferencing .....                    | <a href="#">150</a>                                                                       |  |
| truststore .....                                           | <a href="#">1231</a>                                                                      |  |
| turn off compatibility mode .....                          | <a href="#">45</a>                                                                        |  |
| Turn On Mute .....                                         | <a href="#">772</a>                                                                       |  |
| Turn On Mute for Remote Off-hook Attempt .....             | <a href="#">772</a>                                                                       |  |
| two-way TLS .....                                          | <a href="#">1504</a>                                                                      |  |
| Two-way TLS .....                                          | <a href="#">1503</a>                                                                      |  |
| two-way TLS; configure notify sync .....                   | <a href="#">1501</a>                                                                      |  |
| two-way TLS in System Manager .....                        | <a href="#">1504</a>                                                                      |  |
| <b>U</b>                                                   |                                                                                           |  |
| UCM                                                        |                                                                                           |  |
| synchronize .....                                          | <a href="#">977</a>                                                                       |  |
| UCM and Application Server System Configuration template   |                                                                                           |  |
| field descriptions .....                                   | <a href="#">1154</a>                                                                      |  |
| UDP .....                                                  | <a href="#">828</a>                                                                       |  |
| field description .....                                    | <a href="#">827</a>                                                                       |  |
| UDP entries                                                |                                                                                           |  |
| add .....                                                  | <a href="#">828</a>                                                                       |  |
| edit .....                                                 | <a href="#">828</a>                                                                       |  |
| update .....                                               | <a href="#">829</a>                                                                       |  |
| view .....                                                 | <a href="#">828</a>                                                                       |  |
| UDP field descriptions .....                               | <a href="#">827</a>                                                                       |  |
| UDP Group                                                  |                                                                                           |  |
| deleting .....                                             | <a href="#">825</a>                                                                       |  |
| udp groups .....                                           | <a href="#">823</a>                                                                       |  |
| UDP groups                                                 |                                                                                           |  |
| access .....                                               | <a href="#">830</a>                                                                       |  |
| assign permission .....                                    | <a href="#">830</a>                                                                       |  |
| udp groups field description .....                         | <a href="#">825</a>                                                                       |  |
| unassign                                                   |                                                                                           |  |
| tenant administrator .....                                 | <a href="#">1260</a>                                                                      |  |
| unassigning filter profile from serviceability agent ..... | <a href="#">965</a>                                                                       |  |
| UnAssign Roles page .....                                  | <a href="#">369</a>                                                                       |  |
| unassign users                                             |                                                                                           |  |
| roles .....                                                | <a href="#">193</a> , <a href="#">254</a>                                                 |  |
| unconfigure                                                |                                                                                           |  |
| Geographic Redundancy .....                                | <a href="#">119</a>                                                                       |  |
| understanding                                              |                                                                                           |  |
| groups .....                                               | <a href="#">767</a>                                                                       |  |
| uniform dial plan .....                                    | <a href="#">828</a>                                                                       |  |
| Uniform dial plan                                          |                                                                                           |  |
| UDP .....                                                  | <a href="#">988</a>                                                                       |  |
| Uniform Dial Plan field descriptions .....                 | <a href="#">827</a>                                                                       |  |
| Uniform Dial Plan Group                                    |                                                                                           |  |
| deleting .....                                             | <a href="#">825</a>                                                                       |  |
| uniform dial plan group; add .....                         | <a href="#">823</a>                                                                       |  |
| Uniform Dial Plan Group; edit .....                        | <a href="#">824</a>                                                                       |  |
| Uniform Dial Plan Group; view .....                        | <a href="#">824</a>                                                                       |  |
| uniform dial plan groups .....                             | <a href="#">823</a>                                                                       |  |
| uninstalling a Communication Manager patch .....           | <a href="#">1485</a>                                                                      |  |
| uninstalling a license file .....                          | <a href="#">1035</a>                                                                      |  |
| Uninstall License page .....                               | <a href="#">1044</a>                                                                      |  |
| Unknown location host mapping .....                        | <a href="#">1339</a>                                                                      |  |
| unmanage elements .....                                    | <a href="#">923</a>                                                                       |  |
| unrevoking certificates .....                              | <a href="#">1199</a>                                                                      |  |
| update                                                     |                                                                                           |  |
| Appliance Virtualization Platform .....                    | <a href="#">1347</a>                                                                      |  |
| Branch Session Manager .....                               | <a href="#">1399</a>                                                                      |  |
| Communication Manager .....                                | <a href="#">1357</a> , <a href="#">1397</a> , <a href="#">1399</a>                        |  |
| Session Manager .....                                      | <a href="#">1357</a> , <a href="#">1397</a> , <a href="#">1399</a>                        |  |
| Utility Services .....                                     | <a href="#">1399</a>                                                                      |  |
| WebLM .....                                                | <a href="#">1399</a>                                                                      |  |
| Update Entity Class                                        |                                                                                           |  |
| field descriptions .....                                   | <a href="#">1203</a>                                                                      |  |
| update software .....                                      | <a href="#">1357</a> , <a href="#">1397</a> , <a href="#">1399</a>                        |  |
| update static routing .....                                | <a href="#">1373</a>                                                                      |  |
| Update Static Routing .....                                | <a href="#">1386</a>                                                                      |  |
| update System Manager VM .....                             | <a href="#">1374</a>                                                                      |  |
| Update UDP entries .....                                   | <a href="#">829</a>                                                                       |  |
| field description .....                                    | <a href="#">830</a>                                                                       |  |
| Updating a Communication Manager .....                     | <a href="#">1485</a>                                                                      |  |
| updating ESXi host or vCenter certificate .....            | <a href="#">1349</a>                                                                      |  |
| updating Services Port static routing .....                | <a href="#">1360</a>                                                                      |  |
| updating the SAMP/MPC firmware .....                       | <a href="#">1486</a>                                                                      |  |
| Updating UDP entries .....                                 | <a href="#">829</a>                                                                       |  |
| Updating UDP entries field description .....               | <a href="#">830</a>                                                                       |  |
| upgrade .....                                              | <a href="#">1453</a>                                                                      |  |
| 6.3.100 .....                                              | <a href="#">1440</a>                                                                      |  |
| Branch Session Manager .....                               | <a href="#">1393</a> , <a href="#">1394</a> , <a href="#">1405</a>                        |  |
| checklist .....                                            | <a href="#">1394</a>                                                                      |  |
| Communication Manager .....                                | <a href="#">1393</a> , <a href="#">1394</a> , <a href="#">1405</a> , <a href="#">1440</a> |  |
| Communication Manager 6.x .....                            | <a href="#">1453</a>                                                                      |  |
| elements .....                                             | <a href="#">1401</a>                                                                      |  |
| Session Manager .....                                      | <a href="#">1393</a> , <a href="#">1394</a> , <a href="#">1405</a>                        |  |
| System Platform .....                                      | <a href="#">1453</a>                                                                      |  |
| target release .....                                       | <a href="#">1396</a>                                                                      |  |
| Upgrade .....                                              | <a href="#">1404</a>                                                                      |  |
| Communication Manager .....                                | <a href="#">1484</a>                                                                      |  |
| TN boards .....                                            | <a href="#">1478</a>                                                                      |  |
| upgrade 6.x                                                |                                                                                           |  |
| checklist .....                                            | <a href="#">1453</a>                                                                      |  |
| upgrade Communication Manager 5.2.1                        |                                                                                           |  |
| different server .....                                     | <a href="#">1463</a>                                                                      |  |
| same server .....                                          | <a href="#">1463</a>                                                                      |  |
| Upgrade Configuration                                      |                                                                                           |  |
| field descriptions .....                                   | <a href="#">1404</a>                                                                      |  |
| Upgrade Configuration Details .....                        | <a href="#">1405</a>                                                                      |  |
| upgrade jobs                                               |                                                                                           |  |
| deleting .....                                             | <a href="#">1437</a>                                                                      |  |
| editing .....                                              | <a href="#">1437</a>                                                                      |  |

|                                                                |                                                                    |                                                        |                                           |
|----------------------------------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------|
| upgrade jobs ( <i>continued</i> )                              |                                                                    |                                                        |                                           |
| status .....                                                   | <a href="#">1438</a>                                               | user addressing ( <i>continued</i> )                   |                                           |
| upgrade job status .....                                       | <a href="#">1436</a>                                               | add .....                                              | <a href="#">254</a>                       |
| Upgrade job status                                             |                                                                    | User Attribute Options .....                           | <a href="#">386</a>                       |
| Viewing .....                                                  | <a href="#">1437</a>                                               | User Bulk Editor .....                                 | <a href="#">235</a>                       |
| Upgrade Management .....                                       | <a href="#">1392</a> , <a href="#">1428</a> , <a href="#">1439</a> | User Bulk Editor field descriptions .....              | <a href="#">235</a>                       |
| User Settings .....                                            | <a href="#">1291</a>                                               | User Bulk Import Profile .....                         | <a href="#">892</a>                       |
| Upgrade management workflow summary .....                      | <a href="#">1451</a>                                               | user certificate authentication                        |                                           |
| upgrade media gateways .....                                   | <a href="#">1478</a>                                               | provisioning .....                                     | <a href="#">1243</a>                      |
| upgrade media modules .....                                    | <a href="#">1478</a>                                               | user-defined templates .....                           | <a href="#">1114</a>                      |
| Upgrade Release Selection .....                                | <a href="#">1396</a>                                               | User Delete Confirmation page .....                    | <a href="#">364</a>                       |
| Upgrade Release Setting .....                                  | <a href="#">1439</a>                                               | user details; view .....                               | <a href="#">224</a>                       |
| upgrades                                                       |                                                                    | user import job                                        |                                           |
| supported protocols .....                                      | <a href="#">1486</a>                                               | cancel .....                                           | <a href="#">399</a>                       |
| Upgrade System Manager .....                                   | <a href="#">1426</a>                                               | delete .....                                           | <a href="#">399</a>                       |
| Upgrade to release .....                                       | <a href="#">1396</a>                                               | schedule .....                                         | <a href="#">397</a>                       |
| upgrading                                                      |                                                                    | User Management                                        |                                           |
| Branch Session Manager instances in bulk .....                 | <a href="#">1425</a>                                               | assigning permissions .....                            | <a href="#">202</a>                       |
| upgrading CM Agent template .....                              | <a href="#">1115</a>                                               | roles .....                                            | <a href="#">202</a>                       |
| upgrading CM Endpoint template .....                           | <a href="#">1115</a>                                               | User Management field descriptions .....               | <a href="#">292</a>                       |
| Upgrading Communication Manager 5.2.1 .....                    | <a href="#">1464</a> , <a href="#">1472</a>                        | User management for Application Enablement Services .. | <a href="#">157</a>                       |
| upgrading Communication Manager 5.2.1 to 6.3.100 .....         | <a href="#">1474</a>                                               | User management for Conferencing .....                 | <a href="#">151</a>                       |
| Upgrading Communication Manager 5.2.1 to release 6.3.100 ..... | <a href="#">1476</a>                                               | User management for IP Office .....                    | <a href="#">156</a>                       |
| Upgrading Communication Manager 5.2.1 to release 6.3.6 .....   | <a href="#">1455</a>                                               | User Preference .....                                  | <a href="#">46</a>                        |
| Upgrading Communication Manager 5.2.1 to release 6.3.7 .....   | <a href="#">1475</a>                                               | user profile                                           |                                           |
| Upgrading Communication Manager 5.x .....                      | <a href="#">1484</a>                                               | create .....                                           | <a href="#">225</a> , <a href="#">226</a> |
| Upgrading Communication Manager 6.x to release 6.3.100 .....   | <a href="#">1456</a>                                               | user profile management .....                          | <a href="#">219</a>                       |
| Upgrading Communication Manager 6.x to release 6.3.6 .....     | <a href="#">1456</a> , <a href="#">1457</a>                        | user profiles .....                                    | <a href="#">954</a>                       |
| upgrading devices                                              |                                                                    | user provisioning rule .....                           | <a href="#">227</a> , <a href="#">613</a> |
| protocol matrix .....                                          | <a href="#">1486</a>                                               | add service to user .....                              | <a href="#">615</a>                       |
| upgrading IP Office endpoint templates .....                   | <a href="#">1143</a>                                               | create user .....                                      | <a href="#">226</a>                       |
| upgrading System Platform .....                                | <a href="#">1453</a>                                               | creating .....                                         | <a href="#">616</a>                       |
| Upgrading TN boards .....                                      | <a href="#">1478</a>                                               | deleting .....                                         | <a href="#">618</a>                       |
| upload                                                         |                                                                    | modifying .....                                        | <a href="#">616</a>                       |
| custom patch .....                                             | <a href="#">1413</a>                                               | viewing .....                                          | <a href="#">617</a>                       |
| upload file to software library .....                          | <a href="#">1309</a>                                               | User Provisioning Rule .....                           | <a href="#">295</a>                       |
| uploading a custom patch .....                                 | <a href="#">1413</a>                                               | User Provisioning Rules .....                          | <a href="#">235</a>                       |
| uploading an audio file in IP Office system configuration      |                                                                    | field descriptions .....                               | <a href="#">618</a>                       |
| template .....                                                 | <a href="#">1148</a>                                               | User Restore Confirmation Page .....                   | <a href="#">368</a>                       |
| uploading custom patch .....                                   | <a href="#">1413</a>                                               | user roles                                             |                                           |
| uploading custom patch field description .....                 | <a href="#">1413</a>                                               | view .....                                             | <a href="#">187</a>                       |
| uploading version.xml .....                                    | <a href="#">1487</a>                                               | users                                                  |                                           |
| UPM .....                                                      | <a href="#">257</a>                                                | assign .....                                           | <a href="#">197</a>                       |
| Usage by local WebLM page .....                                | <a href="#">1062</a>                                               | assign groups .....                                    | <a href="#">251</a> , <a href="#">252</a> |
| usage options .....                                            | <a href="#">831</a>                                                | bulk edit .....                                        | <a href="#">233</a> , <a href="#">235</a> |
| Usage Summary page .....                                       | <a href="#">1061</a>                                               | bulk export .....                                      | <a href="#">383</a>                       |
| user                                                           |                                                                    | filtering .....                                        | <a href="#">247</a>                       |
| assign groups .....                                            | <a href="#">366</a>                                                | manage .....                                           | <a href="#">219</a>                       |
| user account                                                   |                                                                    | search .....                                           | <a href="#">249</a>                       |
| create .....                                                   | <a href="#">225</a>                                                | user search                                            |                                           |
| remove .....                                                   | <a href="#">232</a>                                                | searchable fields .....                                | <a href="#">248</a>                       |
| user addressing                                                |                                                                    | User settings                                          |                                           |
|                                                                |                                                                    | configure .....                                        | <a href="#">1287</a>                      |
|                                                                |                                                                    | User Settings                                          |                                           |
|                                                                |                                                                    | field description .....                                | <a href="#">1291</a>                      |
|                                                                |                                                                    | user settings for upgrades .....                       | <a href="#">1287</a>                      |
|                                                                |                                                                    | user synchronization datasource                        |                                           |
|                                                                |                                                                    | field descriptions .....                               | <a href="#">85</a>                        |



|                                                                    |                      |                                                                     |                      |
|--------------------------------------------------------------------|----------------------|---------------------------------------------------------------------|----------------------|
| user synchronization job                                           |                      | view (continued)                                                    |                      |
| create .....                                                       | <a href="#">91</a>   | secondary server alarms .....                                       | <a href="#">997</a>  |
| schedule .....                                                     | <a href="#">92</a>   | subscriber templates .....                                          | <a href="#">1123</a> |
| user synchronization jobs                                          |                      | user import job details .....                                       | <a href="#">400</a>  |
| delete .....                                                       | <a href="#">93</a>   | view an import global user settings job .....                       | <a href="#">406</a>  |
| user synchronization jobs field description .....                  | <a href="#">93</a>   | view an import global user settings job on the Scheduler page ..... | <a href="#">406</a>  |
| using clear amw all .....                                          | <a href="#">722</a>  | view backup files .....                                             | <a href="#">841</a>  |
| using filters                                                      |                      | View by local WebLM page .....                                      | <a href="#">1055</a> |
| filtering endpoints .....                                          | <a href="#">717</a>  | view certificate detail field descriptions .....                    | <a href="#">1198</a> |
| using native name .....                                            | <a href="#">713</a>  | view completed jobs .....                                           | <a href="#">1099</a> |
| using swap endpoints                                               |                      | view contact list member page .....                                 | <a href="#">279</a>  |
| endpoints; swap endpoints .....                                    | <a href="#">722</a>  | view contents; log harvested files .....                            | <a href="#">1008</a> |
| utility                                                            |                      | view details; log harvesting request .....                          | <a href="#">1007</a> |
| bulk import encryption .....                                       | <a href="#">394</a>  | view details of a global user settings importing job .....          | <a href="#">405</a>  |
| Utility Services                                                   |                      | view details of element .....                                       | <a href="#">916</a>  |
| adding .....                                                       | <a href="#">925</a>  | view details of import job .....                                    | <a href="#">405</a>  |
| rolling back .....                                                 | <a href="#">1322</a> | View Element page .....                                             | <a href="#">936</a>  |
| <b>V</b>                                                           |                      | view endpoint                                                       |                      |
| validating connectivity to local WebLM servers for a product ..... | <a href="#">1051</a> | field descriptions .....                                            | <a href="#">735</a>  |
| Validation                                                         |                      | view endpoint template                                              |                      |
| certificate .....                                                  | <a href="#">1347</a> | field descriptions .....                                            | <a href="#">735</a>  |
| vCenter                                                            |                      | view filter profiles .....                                          | <a href="#">966</a>  |
| add .....                                                          | <a href="#">1381</a> | View Group page .....                                               | <a href="#">170</a>  |
| adding .....                                                       | <a href="#">1378</a> | viewing                                                             |                      |
| add location .....                                                 | <a href="#">1380</a> | alarms .....                                                        | <a href="#">991</a>  |
| deleting .....                                                     | <a href="#">1380</a> | certificate add status .....                                        | <a href="#">933</a>  |
| edit .....                                                         | <a href="#">1381</a> | certificates .....                                                  | <a href="#">1197</a> |
| editing .....                                                      | <a href="#">1380</a> | clusters .....                                                      | <a href="#">803</a>  |
| field descriptions .....                                           | <a href="#">1381</a> | CRL download job .....                                              | <a href="#">1236</a> |
| manage .....                                                       | <a href="#">1380</a> | data encryption status .....                                        | <a href="#">1496</a> |
| remove location .....                                              | <a href="#">1380</a> | department .....                                                    | <a href="#">1260</a> |
| removing .....                                                     | <a href="#">1380</a> | endpoint migration job detail .....                                 | <a href="#">731</a>  |
| unmanage .....                                                     | <a href="#">1380</a> | endpoint migration job history .....                                | <a href="#">731</a>  |
| vCenter certificate update .....                                   | <a href="#">1349</a> | groups .....                                                        | <a href="#">160</a>  |
| VDN                                                                |                      | list of outbound firewall rules .....                               | <a href="#">1174</a> |
| adding dependencies .....                                          | <a href="#">833</a>  | notification status .....                                           | <a href="#">932</a>  |
| vector directory number,                                           |                      | outbound firewall rule status .....                                 | <a href="#">1174</a> |
| vdn .....                                                          | <a href="#">688</a>  | password policy status .....                                        | <a href="#">68</a>   |
| vector directory number list .....                                 | <a href="#">688</a>  | resources for a group .....                                         | <a href="#">160</a>  |
| vector routing table                                               |                      | roles .....                                                         | <a href="#">187</a>  |
| call center; vector routing table .....                            | <a href="#">692</a>  | site .....                                                          | <a href="#">1260</a> |
| vector routing table; add .....                                    | <a href="#">692</a>  | subject names for an entity class .....                             | <a href="#">1207</a> |
| vector routing table; edit .....                                   | <a href="#">693</a>  | subject name validation status for an entity class ....             | <a href="#">1208</a> |
| vector routing table; field description .....                      | <a href="#">694</a>  | syslog servers .....                                                | <a href="#">1385</a> |
| vector routing table; view .....                                   | <a href="#">693</a>  | team .....                                                          | <a href="#">1260</a> |
| vector routing table field description .....                       | <a href="#">694</a>  | tenant .....                                                        | <a href="#">1260</a> |
| vector routing table list .....                                    | <a href="#">692</a>  | trunk group .....                                                   | <a href="#">785</a>  |
| verifying changes to date and time configuration .....             | <a href="#">1529</a> | user provisioning rule .....                                        | <a href="#">617</a>  |
| videos .....                                                       | <a href="#">1536</a> | user roles .....                                                    | <a href="#">187</a>  |
| view .....                                                         | <a href="#">1192</a> | virtual machine report status .....                                 | <a href="#">1376</a> |
| global user settings import job details .....                      | <a href="#">405</a>  | Viewing                                                             |                      |
| grace period .....                                                 | <a href="#">880</a>  | administrative user details .....                                   | <a href="#">75</a>   |
| import global user settings job .....                              | <a href="#">406</a>  | viewing active sessions .....                                       | <a href="#">1250</a> |
| location .....                                                     | <a href="#">1317</a> | viewing agent data                                                  |                      |
|                                                                    |                      | agents; view data .....                                             | <a href="#">659</a>  |
|                                                                    |                      | viewing allocations by features .....                               | <a href="#">1054</a> |

|                                                           |                      |                                                            |                      |
|-----------------------------------------------------------|----------------------|------------------------------------------------------------|----------------------|
| viewing allocations by local WebLM .....                  | <a href="#">1054</a> | viewing job summary .....                                  | <a href="#">94</a>   |
| viewing a messaging profile of a user .....               | <a href="#">267</a>  | Viewing job summary field descriptions .....               | <a href="#">95</a>   |
| viewing an announcement .....                             | <a href="#">673</a>  | viewing license capacity .....                             | <a href="#">1034</a> |
| viewing an audio group .....                              | <a href="#">683</a>  | viewing license capacity of a feature .....                | <a href="#">1050</a> |
| viewing an IP Office endpoint template .....              | <a href="#">1141</a> | viewing list of backup files .....                         | <a href="#">841</a>  |
| viewing announcements .....                               | <a href="#">673</a>  | viewing log details .....                                  | <a href="#">1023</a> |
| Viewing an Off PBX Endpoint Mapping .....                 | <a href="#">790</a>  | viewing loggers for a log file .....                       | <a href="#">1017</a> |
| viewing an SNMP target profile .....                      | <a href="#">960</a>  | viewing notification filter profile .....                  | <a href="#">963</a>  |
| viewing an SNMPv3 user profile .....                      | <a href="#">957</a>  | Viewing Off PBX Configuration Set .....                    | <a href="#">786</a>  |
| viewing associated subscribers                            |                      | viewing peak usage .....                                   | <a href="#">1035</a> |
| viewing subscribers .....                                 | <a href="#">1124</a> | viewing pending jobs .....                                 | <a href="#">1098</a> |
| Viewing a UCM and Application Server Configuration        |                      | Viewing Remote Servers .....                               | <a href="#">1093</a> |
| template .....                                            | <a href="#">1151</a> | viewing replica groups .....                               | <a href="#">1072</a> |
| viewing audio groups .....                                | <a href="#">683</a>  | viewing replica node details .....                         | <a href="#">1074</a> |
| viewing authorization code                                |                      | viewing replica nodes in a replica group .....             | <a href="#">1072</a> |
| authorization code; view .....                            | <a href="#">818</a>  | viewing replication details for a replica node .....       | <a href="#">1074</a> |
| Viewing Automatic Alternate Routing Digit Conversion data |                      | viewing reports .....                                      | <a href="#">1090</a> |
| Automatic Alternate Routing Digit Conversion; viewing     |                      | viewing resources for a group .....                        | <a href="#">160</a>  |
| data .....                                                | <a href="#">796</a>  | viewing server properties .....                            | <a href="#">1036</a> |
| Viewing Automatic Route Selection Digit Conversion        |                      | viewing software library .....                             | <a href="#">1304</a> |
| Automatic Route Selection Digit Conversion; viewing       |                      | viewing subscriber templates .....                         | <a href="#">1123</a> |
| data .....                                                | <a href="#">798</a>  | viewing subscriber templates CMM; field description        |                      |
| viewing automatic route selection toll data .....         | <a href="#">801</a>  | CMM field description .....                                | <a href="#">1135</a> |
| Viewing a VMPro call flow template .....                  | <a href="#">1158</a> | viewing subscriber templates Messaging                     |                      |
| Viewing a VMPro System Configuration template .....       | <a href="#">1155</a> | field descriptions .....                                   | <a href="#">1132</a> |
| viewing AVP host                                          |                      | viewing subscriber templates MM; field description         |                      |
| firewall rules .....                                      | <a href="#">1338</a> | MM field description .....                                 | <a href="#">1137</a> |
| Viewing AVP host                                          |                      | viewing templates                                          |                      |
| license status .....                                      | <a href="#">1336</a> | subscriber .....                                           | <a href="#">1123</a> |
| viewing bulk user edit jobs .....                         | <a href="#">233</a>  | viewing the contents of harvested log files .....          | <a href="#">1008</a> |
| viewing certificates .....                                | <a href="#">1197</a> | viewing the details of a contact in the contact list ..... | <a href="#">276</a>  |
| viewing class of service data .....                       | <a href="#">814</a>  | viewing the details of a private contact .....             | <a href="#">281</a>  |
| viewing class of service group                            |                      | viewing the list of outbound firewall rules .....          | <a href="#">1174</a> |
| class of service group; view .....                        | <a href="#">820</a>  | viewing the outbound firewall rule status .....            | <a href="#">1174</a> |
| viewing CM Agent template .....                           | <a href="#">1117</a> | viewing the password policy status .....                   | <a href="#">68</a>   |
| viewing CM Endpoint templates .....                       | <a href="#">1119</a> | viewing the station profile of a user .....                | <a href="#">264</a>  |
| Viewing contents of the certificate .....                 | <a href="#">1215</a> | viewing the status of security hardening .....             | <a href="#">1167</a> |
| viewing coverage path                                     |                      | Viewing UDP entries .....                                  | <a href="#">828</a>  |
| coverage path; view .....                                 | <a href="#">698</a>  | viewing Uniform Dial Plan Group .....                      | <a href="#">824</a>  |
| viewing coverage time-of-day                              |                      | viewing usage by WebLM .....                               | <a href="#">1051</a> |
| coverage time-of-day; view data .....                     | <a href="#">706</a>  | viewing usage summary .....                                | <a href="#">1054</a> |
| viewing data modules                                      |                      | viewing user provisioning rule .....                       | <a href="#">617</a>  |
| data modules; view .....                                  | <a href="#">805</a>  | viewing user roles .....                                   | <a href="#">187</a>  |
| viewing deleted users .....                               | <a href="#">252</a>  | viewing vector directory number                            |                      |
| viewing details of a log harvesting profile .....         | <a href="#">1006</a> | vector directory number; view .....                        | <a href="#">689</a>  |
| viewing details of a log harvesting request .....         | <a href="#">1007</a> | viewing vector routing table data .....                    | <a href="#">693</a>  |
| viewing details of a user .....                           | <a href="#">224</a>  | Viewing Xmobile Configuration data                         |                      |
| viewing enterprise usage of a license feature .....       | <a href="#">1052</a> | Xmobile Configuration; view data .....                     | <a href="#">791</a>  |
| viewing files in the software library .....               | <a href="#">1307</a> | view last contacted status of the local WebLM servers ...  | <a href="#">1051</a> |
| viewing groups .....                                      | <a href="#">160</a>  | view license capacity .....                                | <a href="#">1034</a> |
| viewing harvested log files in an archive .....           | <a href="#">1006</a> | View Local WebLMs page .....                               | <a href="#">1057</a> |
| viewing hunt group                                        |                      | view location .....                                        | <a href="#">1317</a> |
| hunt group .....                                          | <a href="#">781</a>  | view log details .....                                     | <a href="#">1023</a> |
| viewing identity certificates .....                       | <a href="#">1192</a> | view loggers .....                                         | <a href="#">1017</a> |
| viewing IP Office endpoint profiles .....                 | <a href="#">272</a>  | view logs                                                  |                      |
| viewing IP Office system configuration templates .....    | <a href="#">1145</a> | completed jobs .....                                       | <a href="#">1099</a> |
| viewing job history .....                                 | <a href="#">1386</a> | pending jobs .....                                         | <a href="#">1099</a> |



|                                                        |                          |                                          |                      |
|--------------------------------------------------------|--------------------------|------------------------------------------|----------------------|
| view periodic status of master and local WebLM servers | <a href="#">1052</a>     | VPFM                                     | <a href="#">157</a>  |
| View Private Contact List page                         | <a href="#">289</a>      | VxWorks-based CS 1000 server             |                      |
| View Profile:Alarming UI page                          | <a href="#">877</a>      | configuration                            | <a href="#">140</a>  |
| View Profile:Communication System Management           |                          | <b>W</b>                                 |                      |
| Configuration page                                     | <a href="#">866</a>      | warning                                  |                      |
| View Profile:Configuration page                        | <a href="#">869</a>      | data entry in Excel                      | <a href="#">376</a>  |
| View Profile:GracefulShutdown                          | <a href="#">880</a>      | watch list                               | <a href="#">1535</a> |
| View Profile:HealthMonitor UI page                     | <a href="#">880</a>      | WebLM access                             | <a href="#">1032</a> |
| View Profile:Logging page                              | <a href="#">882</a>      | WebLM overview                           | <a href="#">1031</a> |
| View Profile:Logging Service page                      | <a href="#">884</a>      | WebLM server                             |                      |
| View Profile: Trust Management field description       | <a href="#">890</a>      | deleting                                 | <a href="#">1050</a> |
| View Profile: User Bulk Import Profile page            | <a href="#">892, 893</a> | removing                                 | <a href="#">1050</a> |
| View Profile Inventory page                            | <a href="#">869</a>      | WebLM Server on AVP host                 | <a href="#">1335</a> |
| View profile Messaging field descriptions              | <a href="#">871</a>      | WebLM servers                            |                      |
| View Profile SMGR Element Manager                      |                          | periodic status                          | <a href="#">1052</a> |
| field descriptions                                     | <a href="#">885</a>      | What is an audio group                   | <a href="#">682</a>  |
| View Profile SMGR Element Manager field descriptions   | <a href="#">885</a>      | <b>X</b>                                 |                      |
| View Profile System Manager page                       | <a href="#">874</a>      | XML                                      |                      |
| View Public Contact List page                          | <a href="#">597</a>      | import user                              | <a href="#">379</a>  |
| view replica groups                                    | <a href="#">1072</a>     | XML file                                 |                      |
| View Scheduler Profile page                            | <a href="#">887</a>      | import users                             | <a href="#">580</a>  |
| view secondary server alarms                           | <a href="#">997</a>      | XML for user with core attributes        | <a href="#">587</a>  |
| view shutdown history                                  | <a href="#">1274</a>     | xmobile configuration,                   |                      |
| view shutdown history from web console                 | <a href="#">1274</a>     | endpoints; xmobile configuration         | <a href="#">791</a>  |
| View SNMP Profile page                                 | <a href="#">887</a>      | Xmobile Configuration field description  |                      |
| view the details of a public contact                   | <a href="#">594</a>      | Xmobile Configuration; field description | <a href="#">792</a>  |
| view the details of a user import job                  | <a href="#">400</a>      | xmobile configuration list               | <a href="#">791</a>  |
| View Trust Certificate page                            | <a href="#">1188</a>     |                                          |                      |
| view trusted certificates                              | <a href="#">1187</a>     |                                          |                      |
| view UDP Groups                                        | <a href="#">824</a>      |                                          |                      |
| view user import job on the Scheduler page             | <a href="#">400</a>      |                                          |                      |
| View User Provisioning Rule                            |                          |                                          |                      |
| field descriptions                                     | <a href="#">619</a>      |                                          |                      |
| View WebLM page                                        | <a href="#">882</a>      |                                          |                      |
| virtual machine                                        |                          |                                          |                      |
| create                                                 | <a href="#">1352</a>     |                                          |                      |
| snapshot on Appliance Virtualization Platform          | <a href="#">1342</a>     |                                          |                      |
| virtual machine operations                             |                          |                                          |                      |
| job history                                            | <a href="#">1386</a>     |                                          |                      |
| virtual machine report                                 |                          |                                          |                      |
| aborting                                               | <a href="#">1376</a>     |                                          |                      |
| overview                                               | <a href="#">1375</a>     |                                          |                      |
| virtual machine snapshot using SDM                     |                          |                                          |                      |
| deleting                                               | <a href="#">1342</a>     |                                          |                      |
| Visualization, Performance, and Fault Manager          | <a href="#">157</a>      |                                          |                      |
| VM connection reestablish                              | <a href="#">1374</a>     |                                          |                      |
| VM console                                             |                          |                                          |                      |
| opening                                                | <a href="#">1362</a>     |                                          |                      |
| VM Console                                             |                          |                                          |                      |
| overview                                               | <a href="#">1361</a>     |                                          |                      |
| VM Console field descriptions                          | <a href="#">1363</a>     |                                          |                      |
| VMPPro Call Flow Templates field descriptions          | <a href="#">1161</a>     |                                          |                      |
| VMPPro system configuration Templates                  |                          |                                          |                      |
| field descriptions                                     | <a href="#">1157</a>     |                                          |                      |
| VOA Repeat                                             | <a href="#">776</a>      |                                          |                      |
| voice mail number                                      | <a href="#">753</a>      |                                          |                      |
| Voice Terminal                                         | <a href="#">740</a>      |                                          |                      |